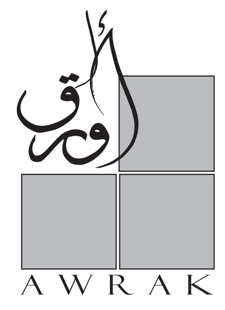


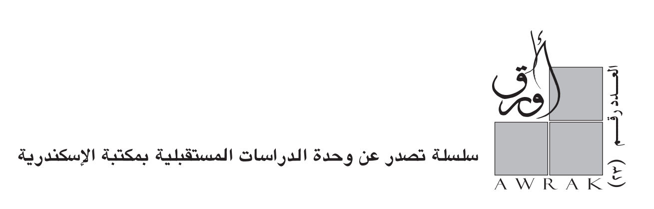
أسلحة الفضاء الإلكتروني
في ضوء القانون الدولي الإنساني

تأليف: عادل عبد الصادق



سلسلة تصدر عن وحدة الدراسات المستقبلية بمكتبة الإسكندرية


أوراق
AWRAK



الآراء الواردة في هذا الكتاب لاتعبّر بالضرورة عن وجهة نظر مكتبة الإسكندرية، إنما تعبّر عن وجهة نظر المؤلف.



سلسلة أوراق

العدد ٢٣

أسلحة الفضاء الإلكتروني
في ضوء القانون الدولي الإنساني

تأليف: عادل عبد الصادق

وحدة الدراسات المستقبلية
مكتبة الإسكندرية

مكتبة الإسكندرية بيانات الفهرسة– أثناء – النشر (فان)

عبد الصادق، عادل.

أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني/ تأليف عادل عبد الصادق. – الإسكندرية، مصر : مكتبة الإسكندرية، وحدة الدراسات المستقبلية، ٢٠١٦.

ص. سم. (أوراق ؛ ٢٣)

يشتمل على إرجاعات ببليوجرافية.

تدمك ١–٣٩٦–٤٥٢–٩٧٧–٩٧٨

١. الفضاء الإلكتروني —قوانين و تشريعات. ٢. الإنترنت — قوانين و تشريعات. ٣. القانون الدولي الإنساني. أ. مكتبة الإسكندرية. وحدة الدراسات المستقبلية. ب. العنوان. ج. السلسلة.

ديوي – ٣٤٣,٠٩٩٤٤ ٢٠١٦٨٢٥٣٩٠

ISBN: 978–977–452–396–1

رقم الإيداع: 2016/22870

المحتويات

مقدمة ٧

المبحث الأول: الفضاء الإلكتروني والتحول في مفهوم الأمن والقوة والصراع العالمي ١١

أولاً: الفضاء الإلكتروني والتحول في الأمن العالمي ١١

ثانيًا: الفضاء الإلكتروني والتحول في استخدام القوة في العلاقات الدولية ١٩

ثالثًا: الفضاء الإلكتروني والتغير في طبيعة وخصائص الصراع الدولي ٣٥

المبحث الثاني: الهيمنة السيبرانية والمزايا الاستراتيجية للأسلحة الإلكترونية ٥١

أولاً: الهيمنة الإلكترونية وإعادة تعريف القوة في العلاقات الدولية ٥١

ثانيًا: خصائص الأسلحة والهجمات الإلكترونية ٥٥

ثالثًا: المزايا الاستراتيجية للتوظيف العسكري للأسلحة الإلكترونية ٦٠

رابعًا: تصاعد القدرات في سباق التسلح السيبراني عبر الفضاء الإلكتروني ٦٤

المبحث الثالث: أثر الفضاء الإلكتروني في القانون الدولي العام وقانون الحرب ٧٧

أولاً: أثر العلم والتكنولوجيا في علم القانون الدولي ٧٧

ثانيًا: مبادئ القانون الدولي الإنساني والفضاء الإلكتروني ٨٢

ثالثًا: هجمات أسلحة الفضاء الإلكتروني واستخدام القوة في العلاقات الدولية ٨٦

المبحث الرابع: تطبيقات القانون الدولي الإنساني على استخدامات الأسلحة الإلكترونية ٩٣

أولاً: مشروعية استخدام هجمات الأسلحة الإلكترونية في حالة النزاع المسلح ٩٣

ثانيًا: مشروعية استخدام هجمات الفضاء الإلكتروني في حالة الدفاع الشرعي ١٠٧

المبحث الخامس: التحديات والإشكاليات في سبيل التعاطي القانوني مع الأسلحة الإلكترونية ١٢١

أولاً: إشكاليات تطبيق القانون الدولي على هجمات الأسلحة الإلكترونية ١٢١

ثانيًا: محددات إعلان الفضاء الإلكتروني نظامًا خاليًا من انتشار الأسلحة الإلكترونية ١٢٥

ثالثًا: محددات تطبيق نظريات الإخلاء والحد من التسلح في الفضاء الإلكتروني ١٣٠

رابعًا: التغير في استراتيجية الردع من العصر النووي إلى الفضاء الإلكتروني ١٣٣

خاتمة الدراسة: نحو خارطة طريق عالمية للتعامل مع الأسلحة الإلكترونية وتأمين الفضاء الإلكتروني	١٤٣
أولاً: الجهود الدولية في سبيل تأمين الفضاء الإلكتروني	١٤٣
ثانيًا: نحو اتفاقية دولية لحماية وتأمين الاستخدام السلمي للفضاء الإلكتروني	١٥٠
التوصيات	١٥٥
نبذة عن المؤلف	١٥٩
قائمة المراجع	١٦١
أولاً: المراجع العربية	١٦١
ثانيًا: المراجع الأجنبية	١٧٠

مقدمة

على مدار التاريخ لعبت القدرة على الاستحواذ على التقدم التكنولوجي دورًا أساسيًّا في قوة الدول وفي ممارسة الهيمنة والسيطرة، وتم نقل تطبيقات ذلك في الاستخدامات المدنية والأخرى ذات الطابع العسكري، وجاء الفضاء الإلكتروني ليدخل كمجال جديد في العلاقات الدولية العابرة للحدود والقادرة على امتلاك منصات القوة الشاملة سواء من قبل الفاعلين من الدول أو من غير الدول.

وجاء المجال الخامس وهو الفضاء الإلكتروني ليشكل مجالاً دوليًّا جديدًا يمثل امتدادًا لنشاط الإنسان ذي الطابع المدني أو العسكري، ويوازي ما يقوم به الإنسان في المجالات والفضاءات الدولية الأخرى؛ كالمجال البري والبحري والجوي والفضاء الخارجي.

واختلف الفضاء الإلكتروني في خصائصه وتحدياته وأنماط استخداماته المدنية والعسكرية، واستتبع ذلك ضرورة التحول من الفوضى إلى التنظيم لعمليات الاستخدام المتعددة له، وهو ما يتطلب البحث على مسارات متكاملة تحقق هذا الهدف، والتي منها ما يتعلق بالأبعاد التقنية والسياسية والإعلامية والاقتصادية والقانونية وغيرها للعمل على تنظيم الاستخدام السلمي للفضاء الإلكتروني، وتحقيق التوزان بين الاستخدامات والواجبات.

ويأتي هذا بعد أن شهد العالم تطورًا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي مع الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف، وأصبحت قضية أمن الفضاء الإلكتروني تلقى اهتمامًا متصاعدًا على أجندة الأمن الدولي، وذلك في محاولة لمواجهة تصاعد التهديدات الإلكترونية ودورها في التأثير على الطابع السلمي للفضاء الإلكتروني، ومحاولة دفع الجهود الدولية لمنع عسكرة المجال الإلكتروني.

وإن كان استخدام القوة في العلاقات الدولية كان قد تم تنظيمه وضبطه في المجال البري أو البحري أو الفضائي، فإن تحول الفضاء الإلكتروني إلى مجال دولي جديد قد فرض كغيره من الظواهر الدولية الجديدة الانتقال من مرحلة الفوضى في الاستخدام إلى التنظيم ومن الحقوق إلى الواجبات.



وبخاصة أنه مع حالة التطور في العلاقة بين العلم والتكنولوجيا والحرب قد فرضت تحديات سابقة في مجال الحد من استخدام الأسلحة التقليدية، أو غير التقليدية وذلك بعد المآسي الإنسانية التي ألمت بالبشرية خلال حربين عالميتين وحروب صغيرة ذات طبيعة داخلية وإقليمية.

فقد كان ذلك الدافع وراء تطوير عصبة الأمم وإنشاء منظمة الأمم المتحدة واعتماد ميثاقها، وإلى جانب ذلك تم تطوير قانون الحرب أو القانون الدولي الإنساني. ومن جهة أخرى تطورت الجهود الدولية للحد من انتشار الأسلحة الكيماوية والبيولوجية والنووية. وعقب ذلك تم كذلك تطوير اتفاقيات دولية للحد من انتشار واستخدام أسلحة محددة في أوقات النزاع المسلح للحد من تأثيراتها العشوائية على المدنيين والمنشآت المدنية، وكذلك الحد من أضرارها على البيئة والمجال الحيوي.

ومن المتوقع أن يشهد القرن ٢١ انتشار استخدام الأسلحة الإلكترونية Cyber Weapons سواء بمفردها أو بالارتباط بأسلحة أخرى، وخاصة في ظل التقدم في مجال الذكاء الاصطناعي والتطور التكنولوجي على مستوى الانتشار والاستخدام عالميًّا، وصعوبة فرض حظر على الأنشطة العسكرية عبر الفضاء الإلكتروني سواء التي تقوم بها دول أو من غير الدول. أو ما يطلق عليهم بالفاعلين الإلكترونيين Cyber Actors. والتطور في أنواع الأسلحة الإلكترونية، وهو ما يظهر في بروز نمط جديد من الصراع الدولي عبر الفضاء الإلكتروني Cyber Conflict. يستخدم الفضاء الإلكتروني إما كوسيط للأعمال العدائية أو كحامل وناقل لحركة التفاعلات الصراعية أو بتحول الفضاء الإلكتروني إلى عنصر هام في القوة العسكرية من خلال تحوله إلى مجال لتطوير الأسلحة الإلكترونية أو السيبرانية Cyber Weapon، والتي تعد شكلاً جديدًا من أشكال الأسلحة.

وفرضت تلك التهديدات الإلكترونية تحديات أمنية جديدة غير تقليدية، وبخاصة مع خبرة المجتمع الدولي في التعامل مع ظهور الأسلحة الكيماوية أو النووية أو البيولوجية وتطوير نظام الأمن الجماعي وفق ميثاق الأمم المتحدة، والقانون الدولي الإنساني أو ما



يعرف بقانون الحرب. ومن ناحية أخرى كشف ذلك عن أهمية البحث عن التعامل مع هذا التحول على نحو مؤسسي وقانوني.

ويمثل البعد القانوني الدولي بعدًا مهمًّا في مواجهة تلك التحديات إذا ما تم تطبيق نظرية المرافق الدولية، على الرغم من أنه ليس الوحيد بل إنه يمثل قوة دبلوماسية وتنظيمية لمحاولة السيطرة والتحكم في الأنشطة غير السلمية عبر الفضاء الإلكتروني، وفرض الاستخدام السلبي للتقدم التكنولوجي تحديات في سبيل معالجة القانون الدولي، وأصبح هناك تأثير متبادل بين التقدم التكنولوجي وما يفرزه من تحديات وقدرة القانون الدولي على التكيف معها، وأصبح هناك تأثيرات على بنية وتفاعلات العلاقات الدولية بشكل عام، أما الأول فهو الانتقال من فضاء قانوني مبني على أساس الجغرافيا إلى فضاء قانوني يحتوي في أحد أبعاده التحلل من الأساس الجغرافي والارتباط بالفضاء الإلكتروني؛ حيث ينتفي مفهوم الحدود بمعناها الجغرافي.

وترتب على هذا التحول أولاً، ضرورة إعادة النظر في ثلاثة مفاهيم، هي مفهوم السلطة القانونية ومفهوم التأثير والنفوذ ومفهوم الشرعية، وثانيًا، كما هي المتغيرات الداخلية والمتغيرات الخارجية في تفاعل الوحدات الدولية إلى درجة أصبح الاختصاص المحلي والاختصاص الدولي أمرًا ليس من اليسير البت فيه. وثالثًا، تجاوز الحدود القضائية وأنه بالنظر إلى منهاجية الدراسة في محاولة البحث في إمكانية تطبيق القانون الدولي على هجمات الفضاء الإلكتروني، فإنه حري بنا أن نستند إلى مصادر ذلك القانون والتي يكون أحد مصادره إذا لم يتم إيجاد موقف قانوني واضح منها، فإنه يمكن الاستناد إلى العرف الدولي وكذلك القياس وآراء محكمة العدل الدولية بالإضافة إلى آراء الفقهاء وغيرها من المصادر التي تعمل على سد الفراغ التشريعي، وذلك من أجل أن يتم النظر إلى الفضاء الإلكتروني على أنه يجب أن يظل شأنه شأن غيره من المجالات التي يمارس فيها الإنسان نشاطه محكومًا بالقواعد العامة التي تحقق صالح المجموعة الدولية كلها، وأصبح هناك اتفاق عام على سريان أحكام القانون الدولي على ما تمارسه الدول أو غير الدول لأي أنشطة داخل النظام الدولي باعتبار أن القانون الدولي قانون عام وعالمي التطبيق، وتكون القواعد القانونية التي لا تطبق هي



تلك القواعد الخاصة بالقانون الدولي التي تحكم مجالات معينة على وجه التحديد، والتي لا يصح تطبيقها على الفضاء الإلكتروني لتعارض طبيعته هذه المجالات وطبيعة وخصائص الفضاء الإلكتروني.

وفي محاولة البحث عن حدود وآفاق وتحديات تطبيق القانون الدولي الإنساني على استخدامات الأسلحة السيبرانية – الإلكترونية في الصراع الدولي، والبحث عن مدى المشروعية، قام الباحث بتقسيم دراسته إلى عناصر تحاول أن تقدم إجابة على تساؤلات رئيسية، وهي مدى مشروعية استخدام الأسلحة السيبرانية – الإلكترونية في النزاع الدولي؟ وما علاقة ذلك بمبدأ منع استخدام القوة في العلاقات الدولية؟ وما تأثير الفضاء الإلكتروني في القانون الدولي العام؟ وما تأثير الفضاء الإلكتروني في التحول في الأمن والقوة والصراع العالمي؟ وما طبيعة الهيمنة السيبرانية والمزايا الاستراتيجية لاستخدام الأسلحة الإلكترونية؟ وما أثر الفضاء الإلكتروني في القانون الدولي العام وقانون الحرب؟ وكيف يمكن تطبيق القانون الدولي الإنساني على هجمات أسلحة الفضاء الإلكتروني؟ وكيف يمكن اعتبار الأسلحة الإلكترونية استخدامًا للقوة في العلاقات الدولية؟ وما مشروعية استخدام الأسلحة الإلكترونية في النزاع المسلح؟ وما مشروعية استخدام الأسلحة الإلكترونية في الدفاع الشرعي عن النفس؟ وما التحديات أمام التعاطي القانوني الدولي مع الأسلحة الإلكترونية؟ وما مستقبل التعامل الدولي مع الأسلحة الإلكترونية وتأمين الفضاء الإلكتروني؟

المبحث الأول

الفضاء الإلكتروني والتحول في مفهوم الأمن والقوة والصراع العالمي

أولاً: الفضاء الإلكتروني والتحول في الأمن العالمي

بعد أحداث ١١ سبتمبر ٢٠٠١ بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد بفعل أحداث دولية، كان أبرزها استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة، وفي عام ٢٠٠٧ برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين إستونيا وروسيا، وفي ٢٠٠٨ في الحرب بين روسيا وجورجيا، وجاء الهجوم الإلكتروني بفيروس ستاكسنت على برنامج إيران النووي عام ٢٠١٠ ليمثل نقلة مهمة بالتطور في مجال الأسلحة الإلكترونية.

وعلى الرغم من الدور السياسي الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في مطلع عام ٢٠١١ فإنها مثلت نقطة هامة لدعم الاهتمام الدولي بأمن الفضاء الإلكتروني، وبرزت محاولات للسيطرة عليها بعد تصاعد الاحتجاجات في أكثر البلدان ديمقراطية وهي بريطانيا والولايات المتحدة. وعلى الرغم من سعي الجيوش النظامية لاستغلال تفوقها التقني العسكري الإعلامي الكاسح، لحسم حرب نظيفة سريعة تجنب السكان فظائع وآلام المواجهة، فإن استراتيجية الشبكات الإلكترونية المسلحة المقاومة لها هي الاستخدام المعاكس لهذه الميزات التقنية، إلى جانب اتباع استراتيجية مواجهة متدرجة تؤدي إلى إنهاك الخصم للتغلب عليه بالتسلل إلى وسط السكان والاحتماء بهم وزعزعة ثقتهم في مؤسسات الدولة، وبالتالي تحويلهم إلى أرضية مواجهة بديلة عن المواجهة المباشرة بين دول، ويتم في ذلك توجيه سلاح الصورة إلى مآسي الحرب وجرائمها الإنسانية بما يعمل على شحن الرأي العام، وهو ما برز بظهور فكرة «إسقاط النظام من الداخل» بدلاً من استخدام القوة العسكرية الخارجية كحالة العراق.

وفي هذا المشهد تنمحي الفروق التقليدية بين الحرب والسلم، ففي الوقت الذي يغدو فيه الصدام السمة الغالبة على الوضع الاستراتيجي الدولي فإنه أفرز تعاونًا متبادلاً، وإن كان نادرًا ما يتطور إلى حالة مواجهة مسلحة للوعي المتزايد بعدم قدرة الحسم العسكري في إطفاء بؤر التوتر القائمة. وتم توظيف التطرف ذي الخلفيات الدينية أو القومية لتحويل استخدام التكنولوجيا من أداة مدنية إلى أداة عسكرية وذات أبعاد تخريبية.

إذا كان الأمن القومي يُعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء الإلكتروني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم العسكري أو الإرهابي، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للأعمال العدائية من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات[١].

وظهرت العلاقة ما بين الفضاء الإلكتروني والأمن الدولي، حيث يوجد المحتوى المعلوماتي العسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي في الفضاء الإلكتروني، خاصة مع التوسع في تبني الحكومات الإلكترونية من جانب العديد من الدول، واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم، حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي، وهذا مما يعرضها لخطر التعرض لهجمات الفضاء الإلكتروني، إلى جانب الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة الداخلية للنظام الحاكم وراء تقديم الدعم المادي والمعنوي عبر الفضاء الإلكتروني. ويُعَدُّ الأمن Security مفهومًا واسعًا يتعلق بتلك الدرجة التي تمكِّن الدولة من أن تصبح في مأمن من خطر التعرُّض للهجوم العسكري أو الإرهابي.

(١) Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007): 1-14.

وتعني كلمة الأمن في مجال الفضاء الإلكتروني: إجراءات الحماية ضد التعرُّض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات. ومن جهة أخرى فإن الأمن القومي يُعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها وغياب الخوف من خطر تعرُّض هذه القيم للهجوم. وتشير كلمة الأمن إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات.

وتعرفه وكالة الأمن القومي في الولايات المتحدة بأنه يعني «المعايير والإجراءات المتخَذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بها عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات».

وأصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، والتي تشمل الطاقة والاتصالات والنقل والخدمات الحكومية والتجارة الإلكترونية والمصارف والمؤسسات المالية، وحيث جعل الفضاء الإلكتروني من تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة، والتي تعرف بالبنية التحتية القومية للمعلومات (NII)، ومن ثم فإن أي هجوم على إحدى تلك المصالح أو كلها يمثل سببًا ومدعاة لحدوث عدم توازن استراتيجي، بما يكشف في الوقت نفسه عن شكل جديد من أشكال الصراع[٢].

ويتعرض الفضاء الإلكتروني لثلاثة أنواع من المخاطر: الكوارث الطبيعية، أخطار عامة، مخاطر إلكترونية. ودخل الأمن الإلكتروني ضمن الأبحاث والدراسات الاستراتيجية. وتتمثل متطلبات توافر الأمن الإلكتروني الدولي في اختبار سلامة الدفاعات الإلكترونية، التأكد من سلامتها، عدم تعرُّضها لأي خلل فني طارئ، ألا تعالَج هذه المسألة منفصلة عن غيرها وإنما من ضمن ترسانة شاملة للدفاع تشكل إطارًا رادعًا لأي حرب استباقية[٣].

---

(٢) Richard K. Betts, *Conflict after the Cold War: Arguments on Causes of War and Peace*, 2nd ed. (New York: Longman, 2002): 548-557.

(٣) مصطفى علوي، «مفهوم الأمن في مرحلة ما بعد الحرب الباردة»، في **أبحاث المؤتمر الذي عقده مركز الدراسات الآسيوية ٤–٥ مايو ٢٠٠٢: قضايا الأمن في آسيا**، تحرير هدي ميتكيس، والسيد صدقي عابدين (القاهرة: كلية الاقتصاد والعلوم السياسية. مركز الدراسات الأسيوية، ٢٠٠٤):١٤.

وباتت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الاستراتيجية – ذات الطبيعة الإلكترونية – إلى أخطار إلكترونية، وتهدد بتحول الفضاء الإلكتروني لوسيط، ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف ودورها تغذية التوترات الدولية، وهو ما يفرض تحديات تتعلق بإعادة تعريف الأمن والقوة والصراع(٤).

وشهد المجتمع الدولي صعود قضايا الأمن الإنساني المشترك. والتغير في المجال الاقتصادي والاعتماد المتبادل وضعف دور الدولة وبروز الفاعلين من غير الـدول(٥). وصاحب ذلك التغير موجة انتشار هائلة لتكنولوجيا الاتصال والمعلومات والتي انتشرت من حيث الكم بمعدلات غير مسبوقة، ومن الناحية الوظيفية دخلت بكثافة في عمل العديد من المرافق الحيوية، والارتفاع الكبير في الجريمة الإلكترونية والقرصنة التي أصبحت تكلف الاقتصاد العالمي ما يزيد على ٢٣٠ مليار دولار سنويًّا، ويتعرض الفضاء الإلكتروني إلى ١٠٠٠ هجوم كل دقيقة، وتنامي حالات الاختراقات الإلكترونية التي تتم بين الفرقاء عبر الفضاء الإلكتروني من دول وأفراد وجماعات، بالإضافة إلى التطور الملحوظ في امتلاك دول لقدرات تطوير واستخدام الأسلحة الإلكترونية، وهو ما يجعل تلك التهديدات تمثل خطرًا على أمن الفضاء الإلكتروني باعتباره أصبح مرفقًا دوليًّا.

وجاءت تلك المظاهر لتبرز استخدامات غير سلمية للفضاء الإلكتروني، وما يمثله ذلك من تهديد للأمن الإلكتروني العالمي والبنية التحتية الكونية للمعلومات من جانب كافة الفاعلين في مجتمع المعلومات العالمي، وأصبح من الممكن لأي طرف متصل بشبكة تكنولوجيا الاتصال والمعلومات أن يتأثر إما بالأطراف الأخرى المتصلة على الشبكة نفسها أو بطبيعة الأخطار التي تعترض هذه الشبكة وتهدد طبيعة عملها، بما يكون له من انعكاسات اقتصادية وأمنية وبما يؤثر على الاستقرار السياسي والاجتماعي، ويعكس ذلك الإيمان القوي بأن الثقة والأمن هما محوران مهمان لمجتمع المعلومات العالمي. وأصبحت مسألة الدعم الفني والتشريعي وتوفير جوٍّ مناسب لانتشار واستقرار البيئة التكنولوجية من أهم مرتكزاته.

(٤) المرجع السابق: ١٣.
(٥) المرجع السابق: ١٥.

يهدد الاستخدام غير السلمي للفضاء الإلكتروني كلاًّ من الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية لمعلومات. وأصبح هناك مصلحة قُطريَّة فضلاً عن دولية في الحفاظ على أمن الفضاء الإلكتروني، على اعتبار أن أمن الدول جزء من الأمن الجماعي، والذي يمكن أن يعمل على ضمان الثقة والأمن والرقابة على شبكات المعلومات والاتصال. ومن هذا المنطلق هناك عدد من الآليات للتعامل مع هذه الأخطار.

وبناءً على حالة التغيير العالمي في المخاطر لعام ٢٠١٦ والتي منها خطر تعطيل البنية التحتية الكونية للمعلومات، من ثَمَّ يصبح من المحتم ألا يعني تحقيق مكاسب لطرف حدوث خسائر لطرف آخر. كما أن حدوث تقدُّم في مجال المكافحة – حتى لو كان جزئيًّا – يصب مباشرة في مصلحة جميع الدول؛ حيث إنه هناك حالة من الاعتماد المتبادل بين جميع الدول حول استخدام بنية تحتية واحدة تنتشر في جميع دول العالم، وترتبط ببعضها البعض، وتمثل مصالح استراتيجية للمجتمع الدولي. وهذا ما يشكل أرضية مهمة لجعل البنية التحتية الكونية للمعلومات أكثر أمنًا واستقلالاً.

إن الهجمات ضد البنية التحتية الكونية للمعلومات لطرف يمكن أن تؤدي بالتبعية إلى أضرار للأطراف الأخرى. وتُستخدم تلك الهجمات أداة استراتيجية يمكن أن تؤدي إلى التأثير على الإتاحة والثقة والأمان والتكامل لأنظمة المعلومات، والتي يمكن أن تُعد على المستوى النظري عملاً من أعمال الحرب، ويمكن أن تدخل ضمن اتفاقيات الحدِّ من التسلح أو قانون النزاعات المسلحة الدولية. ومن ثَمَّ فإن وجود الآليات والوسائل – مثل قانون النزاع المسلح – يمكن أن يتم تطبيقه على تلك الأنواع الجديدة من الأسلحة التي يمكن أن تستخدمها الدول أو الجماعات الإرهابية.

وتواجه مسألة الأمن وتطبيقه في عصر المعلومات بإمكانية استخدام الفضاء الإلكتروني استخدامًا عسكريًّا، وتطوير أدوات حرب المعلومات في مقابل الاستخدام المدني الذي يرتبط بالبنية التحتية للمعلومات وصعوبة الفصل بينهما. وأصبحت قضية أمن الفضاء الإلكتروني قضية دولية تتطلب استراتيجية مرنة تتواءم مع المتغيرات المستمرة، سواء في



الآليات أو في التكتيكات الخاصة بالأمن مقابل التطور المستمر في الأخطار. ويرجع ذلك إلى الطبيعة المتغيرة للفضاء الإلكتروني وفقًا للعامل الإنساني.

وكان لظهور الفضاء الإلكتروني، الذي أخذ في التطور والانتشار الهائل تأثير واضح على شئون الأمن الدولي في حالة استخدامه، وحدث تداخل بين البعد الأمني مع الجنائي مع الطبيعة الدولية للفضاء الإلكتروني. وعلى الرغم من طابعه الافتراضي بالمقارنة بالطبيعة المادية فإنه يعبر عن وجود مادي بشكل خاص، وخصائص مختلفة عن الطبيعة الفيزيائية، ويكون الفاعلون به غير مقيدين بالموقع الطبيعي أو الجغرافي أو الحدود السياسية للدول، وتصبح الأهداف والعناصر غير قابلة للخضوع والسيطرة من الدول وفق معطيات الفضاء الإلكتروني.

وتحوَّل الفضاء الإلكتروني إلى أداة عالمية لتبادل المنافع والمعلومات والمشاركة في إنتاجها عالميًّا، سواء من قِبل الأفراد أو المؤسسات، وشكَّل ذلك خرقًا للمفاهيم التقليدية الخاصة بفكرة القومية؛ حيث تمدد الفضاء الإلكتروني بشكل تجاوز الحدود التقليدية للدول، وكذلك أجواءها الخارجية عبر الأقمار الصناعية، وفقدت الحكومات السيطرة على انسياب المعلومات والأفكار من الداخل وإليه.

واتجهت أدوات تكنولوجيا الاتصال والمعلومات للاندماج في وظائفها وفي درجة تفاعلها كالكمبيوتر والتليفزيون والهاتف المحمول والأقمار الصناعية وشبكات الإنترنت. وأعطت الفرصة لكل فرد حقَّ الدخول والمساهمة والمشاهدة والتفاعل عبر شاشات الكمبيوتر. وأصبح الفضاء الإلكتروني يتسع لجميع أنحاء العالم، في ظل تراجع دور الدولة سياسيًّا واقتصاديًّا وثقافيًّا وفقدانها السيطرة على مواطنيها مع السماوات المفتوحة والفضاءات، وضعف احتكار الدولة للقيم الثقافية أو التعبير عنها أو حتى بثِّ قيم الولاء.

ويشهد العديد من الدول عمليات خصخصة لمرافق كانت في السابق من المرافق الاستراتيجية بهدف تشجيع الاستثمار الأجنبي والقطاع الخاص، إلا أن ذلك حمل معه مخاطر تتعلق بإمكانية تعرُّض تلك المرافق لهجمات، بعد أن أدى ذلك لخروج قطاعات

كانت تُعَدُّ في السابق من ركائز الأمن القومي من سيطرة الدولة. ويؤدي عدم وجود أي رقابة على تلك القطاعات من جانب الدولة إلى أن تكون عرضة أكثر من غيرها للتعرُّض لهجمات إرهابية إلكترونية، وبما يكون له تأثير على الاقتصاد الكلي، وخاصة مع بروز فاعلين من غير الدول وتغيُّر طبيعة الاعتبارات الجغرافية والجيوسياسية مع التطورات المتسارعة في وسائل الاتصالات. وأصبحت البيئة الدولية الجديدة تفرض تغيُّرًا على طبيعة الأولويات والضرورات الدولية. وتعلق الأمن الإلكتروني بطريقة البحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها.

وأدى تصاعد حجم الأخطار الإلكترونية في تغير في مضامين الأمن القومي للدول، وأصبحت تبحث عن إعادة تعريف لأمنها القومي مع ظهور جبهة الفضاء الإلكتروني كمهدد لأمن الدول، وهو ما دفع الدول إلى إدخاله ضمن استراتيجيات الأمن القومي لديها، والبحث عن تطوير قدراتها في مجال الدفاع والحماية والهجوم وتحديث جيوشها للتعامل مع الحرب الإلكترونية الجديدة؛ وهو ما أثر على العلاقات الدولية وبخاصة مع بروز تهديدات من جانب من هم ليسوا بدول وغير مخاطبين بالقانون الدولي، ولا تملك الدول السيطرة كاملة على أنشطة القراصنة أو جماعات الاحتجاج الإلكتروني، حيث أثر الفضاء الإلكتروني على التنافس بين الدول في مجال الاستحواذ على القوة الإلكترونية، وفي نفس الوقت فتح الباب أمام التعاون لمواجهة الأخطار المشتركة وخاصة أنها بطبيعتها عابرة للحدود.

وأصبح الفضاء الإلكتروني يواجه بتهديدات متصاعدة نتيجة:

أ- ارتباط العالم المتزايد بالفضاء الإلكتروني بما عمل على زيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية.

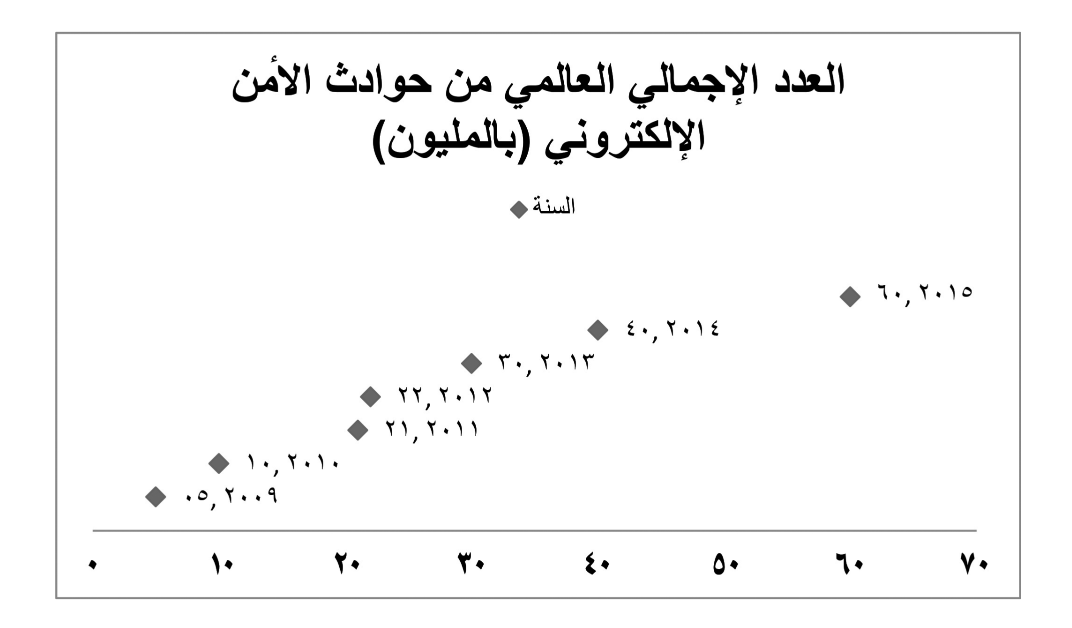
ب- استخدام الفاعلين من غير الدول للفضاء الإلكتروني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.

ج- انسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص وخاصة بالمنشآت الحيوية.



د- تأثير مواجهة الحرب الإلكترونية على حرية استخدام الفضاء الإلكتروني.

هـ- إشكالية تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات، والتي أصبحت فائقة القدرات مثل مواقع الشبكات الاجتماعية كالفيس بوك وتويتر واليويتوب التي أصبحت فاعلة دوليًّا.



المصدر: منتدى الاقتصاد العالمي ٢٠١٥

شكل يوضح تصاعد مخاطر التهديدات الإلكترونية على البنية التحتية الكونية للمعلومات(٦).

(٦) Morgane Fouché, Robert Macrae and Jon Danielsson, "Could a Cyber Attack Cause a Financial Crisis?" *World Economic Forum* (13 June 2016), online e-article, https://www.weforum.org/agenda/2016/06/could-a-cyber-attack-cause-a-financial-crisis.



ثانيًا: الفضاء الإلكتروني والتحول في استخدام القوة في العلاقات الدولية

أ– تعريف وصعود القوة الإلكترونية في الشئون الدولية:

أدت علاقة الفضاء الإلكتروني بعمل المنشآت الحيوية سواء أكانت مدنية أو عسكرية لقابلية تعرضها لهجوم من خلاله، إما يستهدفه كوسيط وحامل للخدمات أو بشل عمل أنظمتها المعلوماتية، ويكون من شأنه التأثير على القيام بوظيفتها، ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب(٧).

وأحدث التطور تحولاً كبيرًا في مفهوم القوة، ترتب عليه دخول المجتمع الدولي في مرحلة جديدة، تلعب فيها هجمات الفضاء الإلكتروني دورًا أساسيًّا سواء في تعظيم القوة أو الاستحواذ على عناصرها الأساسية. وأصبح التفوق في مجال الفضاء الإلكتروني عنصرًا حيويًّا في تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء. واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة(٨).

وفرض الفضاء الإلكتروني إعادة التفكير في مفهوم الأمن القومي، والذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم العسكري أو الإرهابي، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للأعمال العدائية، وأصبح لها تأثير عميق على المجتمع والاقتصاد على النطاق الدولي(٩).

ودخل المجال الإلكتروني ضمن المحددات الجديدة للقوة من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين، وانعكاس ذلك على قدرات الدول وعلاقاتها الخارجية، وتعلقت الخصائص الجديدة للقوة «بأنها مجموعة الوسائل والطاقات والإمكانيات المادية

(٧) عادل عبد الصادق، **الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق** (القاهرة: المكتبة الأكاديمية، ٢٠١٦): ٢٢–٢٦٥.

(٨) Arsenio T. Gumahad, *Cyber Troops and Net War: The Profession of Arms in the Information Age* (Alabama: Air University. Air War College, 1996): 57-156.

(٩) Tim Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet* (London: Routledge, 2000): 160-254.



وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، يستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى»[١٠].

ويغطي مفهوم «القوة الإلكترونية» أو Cyber Power كافة القضايا التي تندرج تحت إطار الصراع الإلكتروني إلى جانب «الحرب الإلكترونية» Cyber War، والتي تشير إلى التطبيقات العسكرية للفضاء الإلكتروني، وتنسيق الهجوم الإلكتروني، والذي يتم شنه من قبل الدولة أو الفاعليين من غير الدول في إطار متبادل أو من طرف واحد، وتعد المعرفة مصدرًا أعلى للسلطة بتقليل الاعتماد على المصادر الأخرى للسلطة ومواردها، وترتبط «السلطة عالية النوعية» بتوافر المعرفة والاستخدام الأمثل لها[١١].

ويرى توفلر أن المعرفة والعنف والثروة هي ثالوث القوة، وتتراوح قدرات الدول على امتلاك الأنماط الثلاثة. وأن الثروة أداة أفضل لممارسة القوة، وأكثرها مرونة؛ حيث تعتمد على المنع والعطاء في الوسط بين أنواع القوة. ولكي تكون القوة أكثر تعبيرًا يجب أن ترتبط بإتقان تطبيق المعرفة، والفاعلية. والمعرفة لا تنضب كما الثروة[١٢].

إذا كانت المعرفة هي القوة فإنها يتم استخدامها من أجل تعزيز القدرة على التأثير في الآخرين لدفعهم لفعل ما تريد، وذلك من خلال ثلاثة طرق رئيسية لتحقيق ذلك: الأولى عن طريق التهديد بالفعل المادي أو الضرب، والطريقة الثانية عن طريق دفعهم بالمكافأة، أما الطريقة الثالثة من خلال اجتذابهم. ويؤكد المفكر الصيني ضن تزو على الأهمية القصوى للمعرفة والدور الأساسي الحاسم لها في الحرب ورابطًا بينها وبين احتمالات النصر في المعركة، وأكد فرنسيس بيكون أن المعرفة هي القوة والسلطة، ويرى جوزيف ناي أن المعلومات تؤثر في القوة وهذه من شأنها أن تجعل نظامًا لا مركزيًّا لتبادل المعلومات بين الدول فيما بين الداخل والخارج. ومن اتجاه الفاعلين الدوليين الآخرين إلى جانب

(١٠) جوزيف س. ناي الابن، **المنازعات الدولية: مقدمة للنظرية والتاريخ**، ترجمة أحمد أمين الجمل، ومجدي كامل (القاهرة: الجمعية المصرية لنشر المعرفة والثقافة العالمية، ١٩٩٧): ٨٢.

(١١) الفين توفلر، **صدمة المستقبل: المتغيرات في عالم الغد**، ترجمة محمد علي ناصف، تقديم أحمد كمال أبو المجد، ط. ٢ (القاهرة: نهضة مصر، ١٩٩٠): ٣٣.

(١٢) الفين توفلر، **تحول السلطة بين العنف والثروة والمعرفة**، ترجمة فتحي حمد بن شتوان، ونبيل عثمان (ليبيا: الدار الجماهيرية، ١٩٩٢): ٤٦٧–٤٨٣.

بروز فاعلين آخرين في الشئون الدولية وتنامي دور المجتمعات المحلية في صنع السياسة الخارجية، ولم تعد الدولة تحتكر عملية صنع السياسة الخارجية.

ووضح ديفلير وركتيش أن قدرة وسائل الاتصال على تحقيق قدر أكبر من التأثير المعرفي والعاطفي والسلوكي، سيزداد عندما تقوم هذه الوسائل بوظائف نقل المعلومات بشكل متميز ومكثف، وتزيد قوة هذا الاحتمال في حالة تواجد عدم استقرار بنائي في المجتمع بسبب الصراع والتغيير. وبقيت فكرة تغيير سلوك ومعارف ووجدان الجمهور يمكن أن تصبح لها تأثير مرتد لتغيير كلٍّ من المجتمع ووسائل الاتصال.

وأصبح الفضاء الإلكتروني[١٣] مجالاً جديدًا للتفاعلات الدولية بشقيها الصراعي والتعاوني، وهو ما أثر في تغير طبيعة القوة من خلال تهديد أمن الفضاء الإلكتروني[١٤]. ويرى والتز أن القوة هي الملاذ الأخير في السياسة الداخلية، أما في السياسة الدولية فإن القوة ليست الملاذ الأخير بل إنها الملاذ الأول والدائم، وهناك عدد كبير من التعريفات حول مفهوم القوة إلا أن أبسطها يصفها بأنها «القدرة على التأثير في سلوك الآخرين». ومن ثم فإن القوة ما هي إلا وسيلة لتحقيق غاية وليست غاية في حد ذاتها، وتسعى الدول إلى تعظيم قوتها وتأثيرها في ظل علاقة التعقد بين الوسائل والأهداف، وأن القوة تعبر عن علاقة بين أكثر من طرفين وليست فاعلاً ساكنًا، وأن القوة نسبية وليست مطلقة، وأن القوة في حد ذاتها عملية وتتم عمليات التأثير عبر الأفعال وردود الأفعال. والتي تعني «بأنها مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، يستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى»، ويعرف جوزيف ناي مفهوم القوة الإلكترونية بأنها تشير إلى «مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل».

---

(١٣) يفضل الباحث استخدام كلمة «الرقمية أو الإلكترونية» بدلاً من كلمة «الافتراضية»؛ حيث يرى الباحث أن الكلمة الأخيرة تعني افتراض وجود شيء ما وتحمل مدلول أنه قد لا يوجد، ولكن في الواقع إن الفضاء الإلكتروني هو وسيط موجود فعلاً وواقعيًا ويتلمسه الناس ودخل في كافة مجالات الحياة.

(١٤) Jordan, *Cyberpower*: 160-254.

ويقدم جوزيف ناي مصطلح «القوة الإلكترونية» لفهم الدور الذي يلعبه الإنترنت في تشكيل قدرة الأطراف المؤثرة، والتي يعد من أبرزها الأطراف الدولية والدول الناشئة، لتحقيق أهدافها. وبأن العصر الإلكتروني قد قلل من صعوبات الدخول، وأعطى الأطراف القدرة والقوة، ولكن القوة الإلكترونية في الوقت نفسه فرضت تحديات كبرى على هؤلاء الأطراف، وخاصة بالنسبة لأطراف ذات تاريخ مثل الولايات المتحدة التي كان لديها ما يشبه الاحتكار لمصادر القوة منذ نهاية الحرب الباردة، ولتظهر عملية انتقال القوة وانتشارها بين أطراف متعددة سواء أكانت دولاً أو من غير الدول.

وأصبح للفضاء الإلكتروني دور فيما يطلق عليه «القوة المؤسسية» في السياسة الدولية، والتي تعني أن يكون لها دور في قوة الفاعلين وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والمساهمة في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، والتي تؤثر في نظريات العلاقات الدولية وتشكيل السياسة العالمية[١٥].

وهناك جدل كبير حول محددات وقدرات القوة الإلكترونية، والتي ترتبط بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها. وهي تعني القدرة على استخدام الفضاء الإلكتروني في خلق مميزات والتأثير في الأحداث التي تجري عبر البيئات التشغيلية، وعبر أشكال وأدوات القوة المختلفة سواء كانت عسكرية أو اقتصادية أو دبلوماسية أو معلوماتية[١٦]، وقد حدد ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية، يتمثل النوع الأول في الدولة، والنوع الثاني في الفاعلين من غير الدول، والنوع الثالث هم الأفراد.

وأدى الفضاء الإلكتروني إلى تغير في طبيعة القوة الراهنة وتغيرت ملامح القوة؛ حيث تم التأكيد أن قياس القوة لا يتم إلا عبر ما يترتب على امتلاك هذه القوة، وبدلاً من سيطرة النظام الحاكم على القوة ومتغيراتها، أتاح الفضاء الإلكتروني الفرصة أمام تعظيم دور أطراف داخلية، مثل الأحزاب أو المجتمع المدني أو الرأي العام في متغيرات القوة الداخلية وامتداد

(١٥) David Held *et al.*, *Global Transformations: Politics, Economics, and Culture* (California: Stanford University Press, 1999).

(١٦) Richard L. Kugler, "From Cyber Space to Cyber Power: Defining the Problems", Chap. 2 in *Cyber Power and National Security*, edited by Franklin D. Krammer, Stuart Starr and Larry K. Wentz, National Defense University Series (Washington, DC: Center for Technology and National Security Policy, 2009): 48.



حجم ومجال تأثيرها إلى خارج حدود الدول، وقوة تأثير المكونات الداخلية على النطاق الدولي والعكس، وأدى الاعتماد المتبادل إلى الترابط بينها، وأصبحت درجة التشبيك من مقومات القوة وتحول بناء القوة من الملكية إلى المعرفة والمعلومات[١٧]؛ وارتفاع أهمية الابتكار والتقدم التكنولوجي في الاستحواذ على القوة، والتي تحولت من على أساس الكم إلى القوة على أساس النتيجة المترتبة عليها. وتحول مفهوم ميزان القوى على أساس الثقل المعادل الذي عبر عنه جنتز في القرن التاسع عشر إلى مفهوم الترابط. والتحول التدريجي للنظر للعلاقات الدولية من علاقات دولية صفرية إلى علاقات دولية غير صفرية.

وأصبحت القوة الإلكترونية حقيقة أساسية في العالم بكل مظاهرها المتنوعة، وبما عمل على دعم ومساندة العمليات الحربية والقوة الاقتصادية والسياسية، وطبيعة النظام الدولي مع التقسيم الدولي للعمل، وتحديد آفاق النمو ومستواه وتوزيع الموارد الاقتصادية وأنماط التفاعل بين القوى الاقتصادية الدولية، والتأثير على القوة السياسية بالتأثير على عمليات صنع القرار في النظام الدولي[١٨].

وتشير «القوة الإلكترونية» إلى القدرة على استخدام الفضاء الإلكتروني لإيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة وعبر أدوات القوة، ومن أهم المتغيرات هو ظهور الاستراتيجية السيبرانية، والتي تشير إلى القدرة على التنمية وتوظيف القدرات للتشغيل في الفضاء الإلكتروني مندمجة وبالتنسيق مع المجال العملياتي الآخر لتحقيق أو دعم إنجاز الأهداف عبر عناصر القوة القومية.

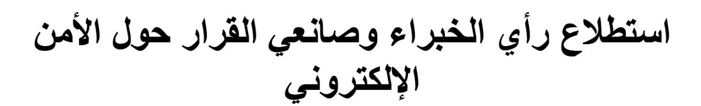
ويقدم جوزيف ناي مصطلح «القوة الإلكترونية» لفهم الدور الذي يلعبه الإنترنت في تشكيل قدرة الأطراف المؤثرة، والتي يعد من أبرزها الأطراف الدولية الناشئة، مثل الولايات المتحدة التي كان لديها ما يشبه الاحتكار لمصادر القوة منذ نهاية الحرب الباردة، ولتظهر عملية انتقال القوة وانتشارها بين أطراف متعددة سواء أكانت دولاً أو من غير الدول[١٩].

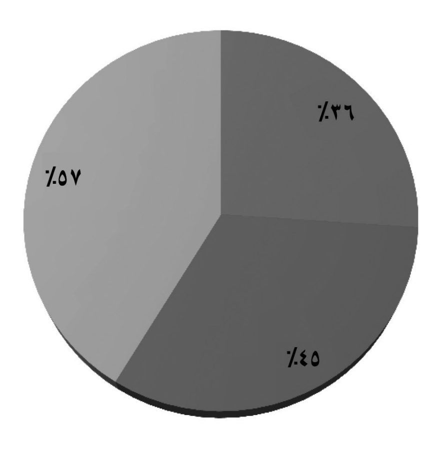
(١٧) وليد عبد الحي، **تحول المسلمات في نظريات العلاقات الدولية: دراسة مستقبلية** (الجزائر: مؤسسة الشروق، ١٩٩٤): ٣٥-٣٨.

(١٨) عادل عبد الصادق، «القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني»، **مجلة السياسة الدولية**، العدد ١٨٨ (إبريل ٢٠١٢).

(١٩) Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011).

ويمكن القول إن عناصر القوة الإلكترونية ترتكز على وجود نظام متماسك يعظم من القوة المتحصلة من التناغم بين القدرات التكنولوجية والسكان والاقتصاد والصناعة والقوة العسكرية وإرادة الدولة، وغيرها من العوامل التي تسهم في دعم إمكانيات الدولة على ممارسة الإكراه، أو الإقناع أو ممارسة التأثير السياسي على أعمال الدول الأخرى، أو على الحكام في العالم بغرض الوصول للأهداف الوطنية من خلال قدرات التحكم والسيطرة على الفضاء الإلكتروني[٢٠].





المصدر: تقرير الدفاع السيبراني، مبادرة أجندة الأمن والدفاع، بروكسيل، بلجيكا، ٢٠١٥

(٢٠) عادل عبد الصادق، «الفضاء الإلكتروني والتحول في سياسات أجهزة الاستخبارات الدولية»، **كراسات استراتيجية**، العدد ٢٤٧ (٢٠١٣): ١٠-١٢.

ب- تأثيرات البعد الإلكتروني في مؤشرات قياس القوة القومية:

أصبح للفضاء الإلكتروني تأثير على القدرة في التأثير على عملية امتلاك الدولة لقدرات القوة عبر التأثير في خصائصها وقدراتها، والتي تعمل على إعادة تشكيل القوة القومية على أسس جديدة يلعب بها البعد الإلكتروني الدور الجوهري في تكوين عناصرها وتماسكها واستمراريتها، وأحدث الفضاء الإلكتروني تغييرًا في قياس القوة بالنظر إلى الموارد بدلاً من التركيز على السلوك، وبدلاً من كون معايير القوة القومية كانت تركز على الموارد الطبيعية بالإضافة إلى المساحة والسكان وغيرها، تم إضافة القدرة على الاستحواذ على القوة الإلكترونية، وأثر الفضاء الإلكتروني على السيادة من خلال تخطية للحدود الدولية، وأثر كذلك على أهمية الموقع الجغرافي والمساحة، وفي إعطاء أهمية أكبر للطابع النوعي للسكان.

وأثر الفضاء الإلكتروني في عناصر القوة القومية من خلال:

• أثر الفضاء الإلكتروني على مصادر وأسس القوة وعناصر القوة، والتي تعد موارد عامة يمكن تطويرها لامتلاك قدرات تسمح بالتأثير، وهو ما يتيحه الفضاء الإلكتروني سواء عبر التطور في التكنولوجيا والأجهزة أو البرمجيات، والتي يمكن أن تعظم من القدرة على التحكم والسيطرة في الفضاء الإلكتروني، وارتباط تلك القدرات بوجود موارد محلية كالمبرمجين والشركات الدولية والقدرة على الابتكار والإبداع والإنفاق على البحث والتطوير وغيرها.

• دور الفضاء الإلكتروني في التأثير في قدرات وأدوات القوة، وذلك من خلال التأثير على الهياكل والمؤسسات المنوطة بها عملية استخدام القوة، والتي قد تشمل القوات المسلحة والأجهزة الاستخباراتية والتطور في الأداء الحربي وتطبيقات التكنولوجيا والتأثير على الدقة في تنفيذ الأهداف وجمع المعلومات وانخفاض التكلفة وقصر زمن التنفيذ. وأدت علاقة الفضاء الإلكتروني بعمل المنشآت الحيوية، سواء أكانت مدنية أو عسكرية لقابلية تعرضها لهجوم من خلاله، إما يستهدفه كوسيط وحامل للخدمات أو بشل عمل أنظمتها المعلوماتية، ويكون من شأنه التأثير على القيام بوظيفتها، ومن ثم فإن التحكم في تنفيذ هذا



الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب. وأحدث الفضاء الإلكتروني تحولاً كبيرًا في مفهوم القوة، ترتب عليه دخول المجتمع الدولي في مرحلة جديدة، تلعب فيها هجمات الفضاء الإلكتروني دورًا أساسيًّا سواء في تعظيم القوة أو الاستحواذ على عناصرها الأساسية.

• أصبح التفوق في مجال الفضاء الإلكتروني عنصرًا حيويًّا في تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء، واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة(٢١). وقد أوجدت ملايين أجهزة الكمبيوتر المنتشرة في كل مكان عالمًا افتراضيًّا نشأ نتيجة عملية الاتصال، ومثّل وسيطًا جديدًا للقوة حيث يمكن للقراصنة دخول الفضاء الإلكتروني بهدف محاولة السيطرة على الأجهزة وسرقة المعلومات وإفسادها أو تعطيلها(٢٢).

• كان يعتمد المقياس التقليدي للقوة القومية للدول بشكل أساسي على مصادر القوة المادية للدولة مثل قدرات الدولة العسكرية. ثم تم طرح القدرات الاقتصادية، وتم طرح منظور شامل لعناصر قوة الدولة من خلال حاصل جمع القدرات النووية والمساحة والسكان، والتقدم الصناعي، والقوة العسكرية. ويرى جوزيف ناي، بأنه لم يعد بالإمكان حساب قوة الدولة، اعتمادًا على العناصر المادية، سواء العسكرية أو الاقتصادية، نتيجة لظهور تهديدات أمنية جديدة مثل الإرهاب، والجرائم الدولية، وتغير المناخ، وانتشار الأمراض المعدية، والتي تتطلب امتلاك موارد القوة الناعمة لمواجهتها(٢٣). وهذا يعني أنه لم يعد كافيًا امتلاك الموارد، سواء كانت مادية أو غير مادية، فلا بد من تحويل هذه الموارد إلى استراتيجية للتأثير على الآخرين، وللحصول على النتائج المرجوة، والمحصلة النهائية لهذه الاستراتيجية هي التي تحدد قوة الدولة(٢٤).

---

(٢١) Gumahad, *Cyber Troops and Net War*: 57-156.

(٢٢) عادل عبد الصادق، «أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني: هل بدأ الاستعداد لحروب المستقبل؟» **السكينة**، http://www.assakina.com/news/news1/9379.html.

(٢٣) جوزيف س ناي، **القوة الناعمة: وسيلة النجاح في السياسة الدولية**: ترجمة محمد توفيق البجيرمي، تقديم عبد العزيز عبد الرحمن الثنيان (الرياض: مكتبة العبيكان، ٢٠٠٤).

(٢٤) Ashley J. Tellis *et al., Measuring National Power in the Postindustrial Age* (California: RAND, 2000): 25-60.

• زاد دور المكون العلمي والتكنولوجي في معدلات القوة والاستحواذ عليها والحفاظ على المكانة الدولية وإلى تغيير موازين القوى بين الدول بناء على ما تمتلكه من مقدرات علمية وتكنولوجية تمكنها من زيادة الناتج القومي الإجمالي لها، وقد تكون صغيرة السكان والمساحة والقوة العسكرية الصلبة كحالة ماليزيا أو سنغافورة بالمقارنة بدول لديها مقدرات قوة قومية كبيرة كالمساحة والسكان والقوة العسكرية، ويعكس حالة التغير في مكونات وعناصر القوة في العلاقات الدولية.

• عكست عملية تغيير طبيعة القوة في العلاقات الدولية طبيعة التغيرات الأفقية والرأسية في النظام الدولي، والتي كان فيها للبعد التكنولوجي والاتصالي دور مهم، سواء على مستوى الثورة في الشئون العسكرية أو فيما يتعلق ببروز مجال جديد للصراع الدولي أو ما يتعلق بانتشار القوة الاقتصادية وانتقال معايير القوة القومية من خصائص السكان والمساحة وعدد الجيش والموارد إلى أبعاد جديدة تتعلق بدور الدولة في الابتكار والإنتاج التكنولوجي، حيث أصبحت دولة مثل سنغافورة لديها ناتج محلي إجمالي يفوق دولاً لديها القوة القومية بالمعايير القديمة، ولم تعد القوى الكبرى تحتكر القوة وحدها مع بروز ظاهرة الاعتماد المتبادل وتعدي الشبكات للحدود الدولية بما فتح المجال أمام لاعبين دوليين جدد، فضلاً عن أن تكلفة الحصول على القوة أصبحت متدنية مع ثورة المعرفة والاتصالات، وهو ما مكن أطرافًا جديدة من الدخول ببساطة للشئون الدولية والتأثير فيها.

• جاء استخدام الفضاء الإلكتروني كنمط من استخدام القوة عن طريق التأثير على عمل مصادر المعلومات وإتلافها وأنظمة الاتصالات عن طريق الهجوم الإلكتروني أو هجوم المعلومات من خلال الأدوات والوسائل الإلكترونية، بما يؤدي إلى شلل هذه الأنظمة وتدمير أنظمة التشغيل الخاصة بها والتأثير على تدفق المعلومات، بما يؤدي إلى إرباك عمل البنية التحتية الحيوية.

• ساعد ظهور الفضاء الإلكتروني على زيادة الدور النسبي للقوة الناعمة في العلاقات الدولية، إما في شكل المعلومات والتأثير على القيم والرأي العام بما يظهر في شكل تغير في السلوك أو عن طريق ووجود أسلحة جديدة ذات طابع إلكتروني تدور عبر الفضاء



الإلكتروني، وتعتمد على المعلومات والابتكار والذكاء البشري. ويتمتع هذا الشكل الجديد من القوة الناعمة بخروجه عن سيطرة الحكومات، حيث إن الفضاء الإلكتروني عابر للحدود ومتاح لاستخدامه من قبل أي فرد.

• أصبح امتلاك القدرة على المساهمة في الثورة المعلوماتية يمثل مفاتيح القوة في العلاقات الدولية، وأصبح يمثل مجالاً لهيمنة الدول بعضها على بعض، سواء بطريقة مباشرة عن طريق السيطرة والتحكم في المقدرات، أو بطريقة غير مباشرة عن طريق القدرة العالية على زرع عملاء في الأجهزة التنفيذية واستخدام تكنولوجيا الاتصال والمعلومات والتقدم التكنولوجي في التجسس. وتحولت القوة العسكرية من قوة النيران إلى قوة المعلومات ثم قوة الذكاء البشري[٢٥].

• أثر الفضاء الإلكتروني على طبيعة الفاعلين في استخدام القوة في العلاقات الدولية، مع الدرجة الكبيرة التي أتاحها في تدفق متزايد للاعبين من غير الدول، وهو ما انعكس على الدور الأمني للدولة، وعمل على مستويين الأول عن طريق إعادة توزيع القوة بين الدولة والفاعلين الآخرين سواء كان بشكل اختياري أو إجباري، وأثر على مستوى بروز قضايا جديدة تتعلق بإعادة تعريف القوة والأمن والصراع وغيرها من المفاهيم المرتبطة، والتي لعب الفضاء الإلكتروني جزءًا كبيرًا في عملها وتطبيقاتها، ومن ناحية أخرى ساهم في التقليل من هامش القوة المتوفر لدى الدولة مقابل أطراف أخرى يمكنها أن تمارس القوة والنفوذ. ودون أن يكون عليها أي إلزام من قبل القانون الدولي كما هو الحال مع الدولة.

• أثر الفضاء الإلكتروني في التقدير الذاتي للقوة لدى الأطراف، حيث إن القوة عبر الفضاء الإلكتروني تتميز بطابعها المستتر وبخاصة ذات الجانب العسكري، ولكن الأخرى تظهر في شكل أدوات الاستحواذ على القوة الاقتصادية والعلمية، ولما كانت القوة التقليدية قابلة للاختبار فإن القوة الإلكترونية يمكن كذلك عن طريقها أن يتم إجراء مناورات إلكترونية للكشف عن الجاهزية والاستعداد والاختبار للقدرات الدفاعية والهجومية عبر

(٢٥) David C. Gompert, Irving Lachow and Justin Perkins, *Battle-Wise Seeking Time-Information Superiority in Networked Warfare* (Washington, DC: Center for Technology and National Security Policy, 2006): 3-13.

الفضاء الإلكتروني، ويدفع التصور الذاتي للأطراف للقوى عبر الفضاء الإلكتروني إلى وجود حالة من التضخم في القوة مستندة إلى البعد الإعلامي في الفضاء الإلكتروني، مثل سعي الولايات المتحدة إلى التضخيم من نشاط تنظيم القاعدة عبر الإنترنت عبر العديد من المواقع والأنشطة، وهو ما يعطي الانطباع بعدم محدودية القوة، وعن إمكانية انفصال تلك القوة المتوهمة عن الواقع.

- تراجع البعد العسكري في تحديد مفهوم القوة عبر الفضاء الإلكتروني، وذلك نتيجة إلى الاعتماد الدولي المتبادل وإلى المخاطر الكبيرة في استخدامها، وعن عملية التقدم في مجال النظم الديمقراطية التي تحد من عملية اللجوء إلى الحرب كحل للصراع[٢٦]. وتم اللجوء إلى أساليب أخرى تركز على الحوار والضغط، ويتم استخدام الفضاء الإلكتروني في الترويج للقيم والأفكار والمصالح للدولة للعمل على توسيع نفوذها العالمي. وتأثيره على تخطي سيادة وحدود الدول بما يعمل على انتشار المهددات غير التقليدية للأمن المتزايد الصلة مع الاقتصاد.

- أثر الفضاء الإلكتروني على وسائل القوة المستخدمة في العلاقات الدولية، والتي يمكن أن تحمل رمزيًّا أو قوة ناعمة وأيضًا القوة الصلبة، مثل: تأثير الفضاء الإلكتروني على القوة العسكرية من خلال تعظيم القدرة على تحسين أداء القوات البرية والجوية والبحرية والتسليح وكفاءتها القتالية والصناعات الحربية، واستخدام الفيروسات الإلكترونية كأسلحة في شن الهجمات أو سرقة المعلومات والحرب النفسية والتأثير في الرأي العام.

- أثر الفضاء الإلكتروني على القوة الاقتصادية من خلال تأثيرها على النمو الاقتصادي وتصاعد دور الاقتصاد الرقمي على حساب الاقتصاد المبني على الموارد الطبيعية، ونمت التجارة الإلكترونية وتمدد نشاط متعددة الجنسيات وعملية انتقال الأموال والثروة عبر الحدود، وأثر الفضاء الإلكتروني في توافر الفرص لتراكم القوة الاقتصادية، وأصبحت لها أهمية غير مسبوقة بسبب تحول الاقتصاد العالمي إلى الاقتصاد الرقمي الذي يساهم

---

(٢٦) جوزيف س. ناي، **مفارقة القوة الأمريكية: لماذا لا تستطيع القوة العظمى الوحيدة في العالم اليوم أن تنفرد في ممارسة قوتها**، ترجمة محمد توفيق البجيرمي (الرياض: مكتبة العبيكان، ٢٠٠٣): ٣٣–٣٥.

وتأثير عملية الابتكار والإبداع والبحث والتطوير في الحفاظ على السوق العالمي وتعزيز الطابع الاحتكاري للشركات الكبرى. وأصبح لأي دول تستطيع أن يكون لها اقتصاد معرفي قوي يجب أن تعمل على تحقيق: أولاً الاستثمار في التكنولوجيا، وبناء شركات تكنولوجية عملاقة، لتكون في كرسي رأس المال، الذي يستفيد بشكل ضخم من هذا التحول العالمي. وثانيًا رفع مستوى التعليم التقني داخل الدولة، بحيث يتحول جزء جيد من الشباب الخريجين إلى موظفين لهم قيمتهم الخاصة في عالم التكنولوجيا. وثالثًا؛ التركيز على الأعمال الإبداعية، لأن الإبداع هو الأمر الوحيد الذي لن تستطيع الآلة فعله عبر السنوات.

• أثر الفضاء الإلكتروني على القوة الدبلوماسية من خلال التأثير في مفهومها وأدواتها ووظيفية الشئون الخارجية. وأثر الفضاء الإلكتروني على الأدوات الاستخباراتية من خلال قدرته على تسهيل عملية جمع وتقييم المعلومات الخاصة بقدرات ونوايا وخطط وتحركات الأطراف الأخرى ذات العلاقة لصالح الدولة والتصنت والتجسس وممارسة وتسهيل النشاطات السرية في العلاقات الدولية، مثل عملية الاغتيال وتزايد العلاقة بين التكنولوجيا والأمن وأثرها على العلاقات بين الدول في ظل ثورة المعلومات والاتصالات والشركات التكنولوجية العابرة للحدود.

• وسهل الفضاء الإلكتروني من تسهيل نشاط الأعمال غير المشروعة، مثل تجارة المخدرات والهجرة غير الشرعية وتجارة السلاح وغيرها، وبالإضافة إلى إتاحة الفرصة إلى تلقي جماعات الجريمة الدعم الخارجي من الخارج بالإضافة إلى دعم نشاطات المعارضة الداخلية بدول أخرى.

• ساهم الفضاء الإلكتروني في تعظيم «الأدوات الرمزية» ودورها في العلاقات الدولية من خلال القدرة على التأثير في أفكار الأطراف الأخرى، سواء على مستوى النخب أو الجماهير من خلال نشر المعلومات والأفكار من أجل توجيه ودعم التأثير في الرأي العام، وممارسة الأعمال العدائية والترويج للسياسات عبر الفضاء الإلكتروني، ودعم عملية التغير الثقافي من خلال سهولة بث المنتجات الثقافية كالأفلام والمسرحيات والتقارير المصورة

والألعاب الإلكترونية. ويمكن استخدام الفضاء الإلكتروني في التأثير في قوة النظم السياسية من خلال التأثير على شرعيته بإحداث الشقة والخلاف بين المجتمع والدولة، وأثر الفضاء الإلكتروني تطوير ونشر برامج كسب التعاطف والولاء عبر برامج تعليم اللغات الأجنبية. أو التدريب أو البعثات الخارجية أو السفر أو الهجرة.

• هناك تصاعد في دور الفضاء الإلكتروني في تنامي النشاطات السرية الدولية في الشرق الأوسط، والتي كان من أبرزها نشاط أقمار التجسس وقيام الموساد الإسرائيلي باختراق أجهزة ونظم الاتصالات في مصر ولبنان وسوريا والعديد من الدول العربية والتجسس عبر الإنترنت والاتصالات، وكانت كلمة السر في عمل التجسس هي كمبيوتر ووصلة نت وشريحة موبيل تعمل بالأقمار الصناعية، فضلاً عن وجود خدمات لأجهزة اتصالات لا تستطيع الدول السيطرة على قاعدة البيانات الخاصة بها مثل الأزمة التي فجرها جهازا بلاك بيري والآيفون، والتجسس على الشبكات الاجتماعية برنامج بيرزيم إلى جانب التجسس عبر الأقمار الصناعية(٢٧).

ج- أنماط استخدام القوة عبر الفضاء الإلكتروني:

تتعدد أنماط استخدام القوة في الفضاء الإلكتروني وفق عدد من المحددات، لعل أهمها ما يتعلق بالمجال الذي تعمل من خلاله. فيتعلق بالنمط الأول أسلحة الفضاء الإلكتروني كعنصر في القوة العسكرية، حيث أصبح التفوق في مجال الفضاء الإلكتروني عنصرًا حيويًّا في تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء. وتعتمد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة.

وقد أوجدت ملايين أجهزة الكمبيوتر المنتشرة في كل مكان عالمًا افتراضيًّا نشأ نتيجة عملية الاتصال، ومثل وسيطًا جديدًا للقوة، حيث يمكن للقراصنة دخول الفضاء الإلكتروني بهدف محاولة السيطرة على الأجهزة وسرقة المعلومات وإفسادها أو تعطيلها. ومع زيادة

---

(٢٧) مثل دور جهاز بلاك بيري في عملية اغتيال «المبحوح» القيادي في حركة حماس بدبي بالإمارات العربية المتحدة، حيث جرى التنسيق للعملية بين عملاء جهاز الموساد الإسرائيلي في يناير ٢٠١٠، وقام المتهمون بتحويلات مالية عبر عدد من شركات الوساطة من خلال حسابات مدفوعة مسبقًا وبطاقات ائتمان بنكية عبر الإنترنت.

اعتماد المجتمعات والجيوش الحديثة على أجهزة الكمبيوتر، أصبح الإنترنت مرادفًا لاستخدام الذكاء الاصطناعي.

والنمط الثاني، يتعلق بتحول الفضاء الإلكتروني كوسيط للأعمال العدائية؛ أصبح الفضاء الإلكتروني وسيطًا للقيام بالأنشطة ذات الطابع المدني والأخرى ذات الطابع العسكري، والتي تجري من خلاله، والتي تعد جزءًا لا يتجزأ من طبيعة العصر الحديث، والتي يتزايد دورها فيما يعرف بالاقتصاد الرقمي والحكومات الإلكترونية والتجارة الإلكترونية، فضلاً عن دورها في وسائل الإعلام والاتصالات الدولية والمصارف والمنشآت الحيوية. ومن ثم فإن أي عملية هجوم قد تستهدف الإنترنت كوسيط وحامل للخدمات وناقل لها من شأنه فشل الإنترنت في القيام بوظيفته، ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب.

والنمط الثالث، يتعلق بأنماط ممارسة القوة عبر الفضاء الإلكتروني «نمط القوة الصلبة» عبر استخدام مقدراته وأدواته في عمل تخريبي عبر قطع كابلات الاتصالات أو تدمير أنظمة الاتصالات أو الأقمار الصناعية أو استخدام الأسلحة الإلكترونية المتقدمة كالفيروسات في تدمير الأنظمة المعلوماتية لمنشآت حيوية بشكل يؤثر على وظيفتها ويهدد أمن الدولة والسكان. وقد تعرضت إستونيا عام ٢٠٠٧ لهجمات إلكترونية، وتم استخدام الهجمات الإلكترونية في الحرب بين جورجيا وروسيا عام ٢٠٠٨.

والنمط الرابع، يتم وفق طبيعة استخدام القوة عبر الفضاء الإلكتروني فيما يمكن أن يطلق عليه «نمط القوة الناعمة»، وذلك بدعم دوره في إدارة العمليات النفسية والتأثير في الرأي العام وتكوين التحالفات الدولية وفي عمل أجهزة الاستخبارات الدولية بما وفره من سيولة للمعلومات عالميًّا لا تقتصر على وجهة النظر الرسمية للدول والحكومات بل تعدى ذلك لدور الأفراد في إنتاج المعلومات وترويجها، وفي توافر كم هائل للتحليلات السياسية والاقتصادية مع تعدي الحدود الدولية، وشكل ذلك ثورة معلوماتية هائلة لا حدود لها



عكفت عليها أجهزة الاستخبارات الكبرى للحصول عليها أولاً، والبحث فيها ثانيًا وتوظيف نتائجها ثالثًا(٢٨).

وهو ما يأتي في إطار استخدام الفضاء الإلكتروني في القيام بحروب غير تقليدية(٢٩) عبر هجمات الإرهاب الإلكتروني وإطلاق فيروسات الحاسب والتجسس الإلكتروني والاختراق المباشر لشبكات المعلومات، ولم تعد أشكال الخطر التي تهدد المحتوى المعلوماتي والمجتمعي المشترك مقصورة على الأشكال التقليدية، بل أصبح لها أوجه رقمية إلكترونية غير مسبوقة في شمولها وعمقها واختلافها واتساع نطاق تغطيتها وفداحة أضرارها وذكاء منفذيها وتعقد آلياتها وتواصل هجماتها وتتضمن أخطار تعقب وجمع المعلومات، والثانية تقوم على إفساد وتعطيل إتاحة المعلومات مثل المعلومات العسكرية والأمنية والاقتصادية والمحتوى الفكري والسياسي والاجتماعي والعلمي.

تعد هجمات شبكات الكمبيوتر والتي يطلق عليها حرب الفضاء الإلكتروني جزءًا من عمليات المعلومات، والتي يمكن أن يتم استخدامها في مستويات ومراحل الصراع المختلفة، سواء كان ذلك على الجانب التكتيكي أو الاستراتيجي أو العملياتي، ويتم استخدام تلك الهجمات في أي وقت سواء أكان وقت سلم أم حرب أم أزمة. وتعرف كليات الحرب الأمريكية الإرهاب الإلكتروني، وتدعوه بهجمات الشبكات الكمبيوترية، وتصنفه تحت بند العمليات الإلكترونية(٣٠). والتي تشير إلى جملة الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها.

وتوجد طرق عديدة يمكن من خلالها تنفيذ الهجمات عبر الفضاء الإلكتروني، منها الهجمات المباشرة من خلال التدمير الفيزيائي لأجهزة الخصم، أو نقاط الاتصالات المهمة

(٢٨) عادل عبد الصادق، «الإنترنت والاتصالات ساحة جديدة للتجسس الدولي»، **قضايا استراتيجية** (يونيو ٢٠١٣)، http://www.accronline.com/article_detail.aspx?id=13513.

(٢٩) Lucas Walsh and Julien Barbara, "Speed, International Security, and "New War" Coverage in Cyberspace", *Journal of Computer-Mediated Communication* 12, no. 1 (Oct 2006): 20-45, online e-article, http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2006.00321.x/full.

(٣٠) Keith B. Alexander, "Warfighting in Cyberspace", *Joint Forces Quarterly* 3, no. 46 (2007): 58-61, online e-article, http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-46.pdf.



ضمن شبكاته، وذلك باستخدام القوة العسكرية المباشرة. وهناك أيضًا سرقة المعلومات من أجهزة الخصم، ومن ثم اتخاذ قرارات أفضل في المعركة، إضافة إلى تخريب قواعد بيانات الخصم والتلاعب بها، لجعل الخصم يخطئ في اتخاذ القرارات. وبالطبع هناك استخدام الفيروسات والأساليب الإلكترونية مثل هجمات الحرمان من الخدمات للتأثير على مواقع الخصم، مما يؤدي إلى التقليل من مقدرة الخصم على الاتصال وإبطاء قدرته لاتخاذ القرار.

وتتضمن هجمات الكمبيوتر حدوث هجوم على خطوط الاتصالات وتأتي تلك الهجمات من مسافة بعيدة عن مصدر الهجوم؛ وذلك عبر الشبكات الدولية للمعلومات العابرة للحدود ومن خلال موجات الراديو أو الشبكات الدولية للاتصالات بدون تدخل مادي أو طبيعي في الأراضي الخاصة بدولة أخرى أو القيام بغزوة تقليدية. وأوجد الفضاء الإلكتروني بيئة استراتيجية فريدة ووسّع من مجالها وبخاصة فيما يتعلق بقيام الفاعلين من الدول أو من غير الدول بالأنشطة العدائية ضد أطراف أخرى.

ويمكن أن تتم تلك الأنشطة عبر ثلاثة أنماط من الفعل، ويتم أولها عبر اختراق أنظمة اتصالات ومعلومات العدو لأغراض التجسس. وهذا ليس في إطار حرب الفضاء الإلكتروني. وثانيها، حرب ناعمة في الفضاء الإلكتروني – هي عمليات في الفضاء الإلكتروني، التي جوهرها إرباك مهمة العدو، مثل الحرب النفسية، وعدم التسبب مباشرة في دمار. وثالثها، حرب الفضاء الإلكتروني – هي عمليات في الفضاء الإلكتروني تشتمل على هجمات موجهة لإحداث ضرر مباشر أو دمار للعدو. بما في ذلك إحداث ضرر لأنظمة الاتصالات والمعلومات أو لأهداف في المجالات المادية ترتبط في عملها بالفضاء الإلكتروني.

د– أبعاد التحول الاستراتيجي في القوة عبر الفضاء الإلكتروني:

البعد الأول: يتعلق بالقيام بعملية استخدام الفضاء الإلكتروني بشكل موجه للمجال البشري، وهدفها تغيير سلوك وتصرفات الشخص المستخدم. من بينها نقل رسائل معلومات علنية وسرية للغريم بواسطة مجال الفضاء الإلكتروني.

البعد الثاني: يتعلق بالقيام باختراقات إلكترونية للبرمجيات وأنظمة المعلومات لأهداف مثل التجسس، ومهاجمة حواسيب طرف لمنع حصوله على موارد ومزايا الفضاء الإلكتروني، إلى جانب شن هجمات على منشآت البنية التحية والتي تعتمد في عملها على الفضاء الإلكتروني.

ويتم ذلك عن طريق التشويش على جهاز التحكم الحراري، الذي يقود لتفجير مصنع أمني (تأثير في المجال البري)، أو إرباك مقياس الارتفاع، الذي يقود لإصابة طائرات (تأثير في المجال الجوي). في هذه الحالة أضحى مجال الغريم الفضاء الإلكتروني أداة في خدمة المُهاجِم، وعليه من شأنه الامتناع عن المساس بأنظمة اتصالات ومعلومات الخصم.

البعد الثالث: في المجال المادي المرتبط بالفضاء الإلكتروني؛ حيث يتم القيام بعمليات من خارج مجال الفضاء الإلكتروني ضد بنى تحتية يعتمد عليها المجال. مثل العمليات النيرانية (الحركية) والحرب الإلكترونية التي تهدف إلى الإضرار أو شل مكوّنات الاتصال وأنظمة الطاقة، المتصلة بمجال الفضاء الإلكتروني.

البعد الرابع: يتعلق بالارتباط بين الفضاء الإلكتروني والمجالات الأخرى مثل المجال البحري والبري والفضاء الخارجي؛ حيث تعمل الأقمار الصناعية الخاصة بالاتصالات والتجسس والتي يمكنها القيام بالتأثير على الموجات الكهرومغناطيسية التي يمكن أن تؤثر على عمل البنية التحتية.

ثالثًا: الفضاء الإلكتروني والتغير في طبيعة وخصائص الصراع الدولي

أ- ماهية الصراع الإلكتروني عبر الفضاء الإلكتروني:

ظهرت العلاقة ما بين الفضاء الإلكتروني والصراع باعتبارها بعدًا جديدًا يتضمن كل شبكات الاتصالات ومصادر المعلومات التي يتم تبادلها إلكترونيًا، والصراع الإلكتروني هو حالة من التعارض في المصالح والقيم يتم تسويته عبر الفضاء الإلكتروني، واتجه الصراع الدولي حول الموارد والمصالح والقيم نحو الاعتماد على تكنولوجيا الاتصال والمعلومات

فيما يعرف بصراع «عصر المعلومات» والتنافس في ساحة الإنجازات ذات الطبيعة المادية وصراع آخر حول الأفكار والقيم[٣١].

ويتميز «الصراع الإلكتروني» Cyber Conflict بأن به تدميرًا لا تصاحبه دماء وأشلاء بالضرورة، يتضمن التجسس والتسلل ثم النسف لكن لا دخان ولا أنقاض ولا غبار، ويتميز أطرافه بعدم الوضوح وتكون تداعياته خطيرة، سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة، للنيل من سلامة تلك المواقع[٣٢].

وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت أيضًا وتعلم كيفية استخدامها، كما أن انتشار الفضاء الإلكتروني وسهولة الدخول إليه يمكن أن يوسع دائرة استهداف المواقع بالإضافة إلى زيادة عدد المهاجمين، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع ممتد يرتبط بطبيعة الفضاء الإلكتروني المختلفة[٣٣].

ودفعت الأهمية المتصاعدة للفضاء الإلكتروني في الاستحواذ على القوة إلى الصراع حول امتلاك مقدراتها وأدواتها من أجل العمل على الحماية والدفاع وتطوير القدرات الهجومية، في سبيل تعظيم القوة والتفوق والهيمنة بين الدول والفاعلين من غير الدول وتعزيز التنافس حول السيطرة والابتكار والتحكم في المعلومات، وتعظيم القدرات القادرة على زيادة النفوذ والتأثير، ليس على نطاق محلي فقط، بل على نطاق دولي أيضًا.

وساهمت تلك المتغيرات في بروز وعي عالمي بما يحدث ودرجة عالية من التأثير والتأثر في أرجاء العالم المختلفة، وأفرز الفضاء الإلكتروني بيئة دولية جديدة تمثلت في إعطاء

---

(٣١) Myriam Dunn, "Information Age Conflicts: A Study of the Information Revolution and a Changing Operating Environment", *Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung*, no. 64 (2002), online e-article, http://kms1.isn.ethz.ch/serviceengine/Files/ISN/55/ipublicationdocument_singledocument/dadc0d4d-948f-4d9d-8b54-fce922e1f152/en/doc_57_290_en.pdf.

(٣٢) Myriam Dunn, "The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method", *Information and Security: An International Journal* 7 (2001): 145-158, online e-article, http://procon.bg/system/files/07.08_Dunn.pdf.

(٣٣) Jennie M. Williamson, *Information Operations: Computer Network Attack in the 21st Century, Strategy* Research Project (Pennsylvania: U.S. Army War College. Carlisle Barracks, 2002): 15-22.



دفعة قوية لزيادة المعرفة في عمليات الإنتاج والابتكار، والأهمية المتزايدة للاتصالات، وهي أحد أوجه الأمن مما جعل هذه البيئة الإلكترونية حقيقة غير مسبوقة، بالإضافة إلى عدم كفاية الاعتماد على القوة العسكرية، وإعادة النظر في تعريف الأمن؛ مع ظهور أوجه غير عسكرية له، وتتأثر حالة الصراع وانعدام الأمن في الفضاء الإلكتروني بكل أنواع البيئات الأخرى غير المتصلة بالفضاء الإلكتروني كالنزاعات بين الأفراد والصراع بين الجماعات والصراع بين الدول أو صراع بين الشركات الدولية، وتعددت أنماط الصراع ما بين صراع ذي طابع قانوني وتجاري أو صناعي وعسكري وسياسي، وامتد تأثير ذلك ليشمل كافة المجالات الأخرى التي تدور على أرض الواقع.

ويتمدد الصراع الإلكتروني بداخل شبكات الاتصال والمعلومات متجاوزًا الحدود التقليدية وسيادة الدول، ويؤثر ذلك في امتداد مجاله وتداعياته أو آثاره، وأضافت عملية تعدد الاستخدام والفاعلين والمصالح لتنوع أشكال الصراع وأهدافه.

ولأن الصراعات «الفعلية» تستعمل شتى أنواع أسلحة التدمير الاقتصادية والإلكترونية والسياسية والإعلامية، فإنها لم تتوانَ عن استخدام الفضاء الإلكتروني، بما له من تأثير نفسي ومعنوي وإعلامي، ثم أصبح له تأثير أمني وعسكري لتزحف جبهات القتال التقليدية بشكل موازٍ لها إلى ساحة الفضاء الإلكتروني[٣٤].

وكشف استخدام الفضاء الإلكتروني عن حالة التعارض الحقيقي أو المتخيل للاحتياجات والقيم والمصالح بين العديد من الفرقاء، سواء أكانوا دولاً أو أفرادًا أو جماعات أو شركات، وبما ساعد على بلورة أساليب للصراع الدولي ذات الطابع التقني والتجاري والاقتصادي والعسكري، إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول أو بين الخصوم عبر شبكات الاتصال والمعلومات[٣٥].

(٣٤) عادل عبد الصادق، «هل يمثل الإرهاب الإلكتروني شكلاً جديدًا من أشكال الصراع الدولي»، **ملف الأهرام الاستراتيجي**، العدد ١٥٦ (ديسمبر ٢٠٠٧).

(٣٥) Andreas Wenger, "The Internet and the Changing Face of International Relations and Security", *Information and Security: An International Journal* 7 (2001): 5-11.

وكان لتلك التغييرات دور في إعادة التفكير في حركية وديناميكية الصراع والأمن على نحو يعكس التطور الذي فرضه الفضاء الإلكتروني على المجتمع الدولي، وخاصة في ظل تزايُد حالة الاعتماد المتبادل، وهو ما ساعد في ظهور ما يعرف بـ «عصر القوة النسبية» الذي يعني بعجز «القوة العسكرية» عن تأمين الأهداف السياسية المترتبة عليها، مما يخلف آثارًا استراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي.

وذلك بعد أن تغير «براديم» الحرب جذريًّا بانتقاله من نسق «الحروب الصناعية بين الدول» إلى نسق «الحرب في وسط الشعوب». ففي الحروب القديمة كان الغرض هو تدمير الخصم، إما باحتلال أرضه أو الاستيلاء على موارده، بينما أصبح في الحرب الجديدة هو التحكم في إرادته وخياراته، ومن ثم كان الدور المحوري للشعوب في هذا الصنف الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في الدولة التي تشن الحرب، أو بالرأي العام الإقليمي والدولي. وأصبحت أهداف الحرب أقل مادية، يؤدي فيها العامل النفسي والدعائي دورًا محوريًّا، وسببه تنامي التغطية الإخبارية السمعية البصرية المباشرة للأحداث لحظة وقوعها عبر مواقع الإنترنت والفضائيات إلى جانب ضعف سيطرة أنظمة الحكم على توجهات مواطنيها.

ومن أهم أشكال الصراع في عصر المعلومات هو حرب الشبكات وحرب الفضاء الإلكتروني Cyber War & Net War، وعلى الرغم من زيادة معدلات استخدام تلك الأشكال فإن ذلك لا يعني بالضرورة اعتمادها فقط وسائل تكنولوجيا الاتصال والمعلومات، بل تأتي مواكبة أو معبرة عن استخدام الآليات التقليدية للصراع ولكن بوجه تكنولوجي يتواكب مع عصر المعلومات[٣٦].

وأصبح الفضاء الإلكتروني ساحة لنقل الصراعات وتصفية الخلافات بشتى أنواعها بين الفرقاء، وفرضت نفسها بقوة على واقع الصراعات المسلحة وغير المسلحة، وأضفت

(٣٦) Athina Karatzogianni, ed., *Cyber-Conflict and Global Politics*, Contemporary Security Studies (London: Routledge, 2008): 240-272.

التقنيات الرقمية ومدى التقدم العلمي بها مزيدًا من الفاعلية على ذلك النوع من الحروب عبر الفضاء الإلكتروني.

وهناك صراع إلكتروني تحركه دوافع سياسية ويأخذ شكلاً عسكريًّا، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني؛ وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية وبما يتضمن استخدام أسلحة وأدوات إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي أو من خلال التعاون ما بين قوى أخرى لتحقيق أهداف سياسية(٣٧).

وهناك صراع إلكتروني ذو طبيعة ناعمة عن طريق الصراع حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية. ويتم أيضًا من خلال تسريب المعلومات واستخدامها عبر منصات إعلامية بما يؤثر على طبيعة العلاقات الدولية كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية(٣٨).

ويأخذ الصراع الإلكتروني طابعًا تنافسيًّا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع، والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول بدون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية كهجمات قراصنة الكمبيوتر وتدمير المواقع والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس قوة تفجير تقليدي مدمر.

وخاصة مع صعوبة الفصل بين النشاط الذي يتعلق بالاستخبارات وجمع المعلومات وحرب الفضاء الإلكتروني أو التمييز بين الاستخدام السياسي والإجرامي، وتساهم البيئة المثالية تلك للفضاء الإلكتروني في عمل الجماعات المختلفة ودعم القدرة على تشكيل شبكة عالمية بدون سيطرة مباشرة بالإضافة إلى رخص التكلفة وسهولة الاتصال وضعف الرقابة التقليدية عليه، ومثّل ذلك عنصر جذب لاستخدامها وتوظيفها لتحقيق أهداف سياسية وعسكرية.

---

(٣٧) Dunn. *Information Age Conflicts*: 2-6.

(٣٨) عادل عبد الصادق، «موقع ويكيليكس وتحدي عالم الاستخبارات الأمريكي»، **ملف الأهرام الاستراتيجي**، العدد ١٩١ (أكتوبر ٢٠١٠).

وساعدت البيئة المحلية والسياق الدولي للفضاء الإلكتروني على بروز الصراعات ذات البعد المحلي – الدولي من خلال توفير بيئة مناسبة لدمج الفئات والقوى المهمشة في السياسة الدولية وخلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض إما على أساس قيم حقوقية أو انتماءات عرقية أو دينية[٣٩]. وساهم الفضاء الإلكتروني في دعم الهيكل التنظيمي والاتصالي للحركات والجماعات والمنظمات المدنية إلى جانب بروز ظاهرة الفاعلين من غير الدول في عمليات التجنيد والحشد والتعبئة والتمويل[٤٠].

وتنتقل الصراعات الممتدة عبر الفضاء الإلكتروني، وتتميز بحدوث حالات متكررة للقرصنة المتبادلة دون أن تسفر عن حرب تقليدية بالضرورة، وخاصة مع صعود دور «الفرد» في العلاقات الدولية، مثل حالة الصراع العربي الإسرائيلي أو ما بين باكستان والهند أو ما بين الصين والولايات المتحدة أو ما بين الصين وتايوان أو كوسوفا أو غيرها من مناطق الصراعات.

ويمكن أن يستخدم الفضاء الإلكتروني كوسيلة من وسائل الصراع داخل الدولة Inte-State Conflict، بين مكوناتها على أساس طائفي أو اقتصادي أو ديني، وهو ما يساعد على كشف ديناميات التفاعل الداخلي إلى الخارج، بما يسهل من عملية الاختراق الخارجي عبر شبكات الاتصال بدعم أحد أطراف الصراع بأدوات غير قتالية.

وبرز دور الفضاء الإلكتروني أيضًا عبر شبكات التواصل الاجتماعي في إدارة الصراع السياسي بين الشركات التكنولوجية الكبرى والدول من ناحية وما بين النظم الحاكمة والحركات المعارضة لها من ناحية أخرى[٤١]، وخاصة في دول الربيع العربي؛ حيث برز تفاوت في استخدام الفضاء الإلكتروني وفق طبيعة التطور التقني وقدرة النظام على إدارة الصراع الإعلامي والتأثير في الرأي العام وتعبئة وحشد الجمهور.

---

(٣٩) ومثال على ذلك التجمعات الإلكترونية على شبكات التواصل الاجتماعي والمنتديات الإلكترونية وتأسيس المواقع الإلكترونية للمنظمات الحكومية وغير الحكومية.

(٤٠) عبد الصادق، «هل يمثل الإرهاب الإلكتروني شكلاً جديدًا من أشكال الصراع الدولي».

(٤١) كان من أشهر تلك الحركات حركة احتلوا وول ستريت والتي انتشر نشاطها في أغلب مساحة الولايات المتحدة وعملت على الاستفادة من النموذج المصري في استخدام تكتيكات الاحتجاج ووسائله وبخاصة التكنولوجية، انظر: *Tumblr. #occupywallstreet*, http://occupywallstreet.tumblr.com.

ويتم استخدام الفضاء الإلكتروني في شن الحرب النفسية على السكان بما يؤثر على درجة استقرار المجتمع مع انتشار استخدامه وزيادة الاعتماد عليها وإتاحتها أمام جميع المستخدمين دون تمييز، ويكون لذلك النوع تأثير على السكان بما يجعلهم يشعرون بالعجز وعدم الثقة في مؤسسات الدولة والاحتماء بالولاءات التقليدية الأولية بما يشكل بداية استخدام الدين والقبيلة والعرق كدوافع من دوافع الصراع، والتي تقوض سلطة الدولة وتطيل أمد الصراع.

وكان للفضاء الإلكتروني دور في وجود أهداف ووسائل ومصالح إلكترونية جديدة، وفي نفس الوقت أتاح القابلية لخطر التعرض للهجوم، وهو ما أوجد نوعًا جديدًا من الضرر دون الحاجة للدخول الطبيعي والمادي لإقليم الدولة، وذلك لاعتماد الدول على الأنظمة الإلكترونية في كافة منشآتها الحيوية بما يجعل من تلك الأنظمة هدفًا للهجوم، وخاصة أن تلك الأنظمة تحمل طابعًا مدنيًّا وعسكريًّا مزدوجًا. وذلك بعد أن تمخض عن الثورة التكنولوجية ثورة أخرى هي الثورة في الشئون العسكرية وتطور تقنيات الحرب(٤٢).

ب- تطبيقات الصراع الإلكتروني في الشأن العالمي:

يمكن تصنيف الفضاء الإلكتروني من حيث تعرُّضه لأنماط الحرب والصراع إلى صراع. وهناك ثلاثة أنماط من الصراع الإلكتروني، يتعلق منها الأول بنمط الصراع منخفض الشدة، وهو الذي يعبر عن سلسلة من الأنشطة العدائية السرية التي لا تتطور إلى حالة التخريب أو التدمير، والنمط الثاني، يتعلق بتحول الصراع الإلكتروني إلى نمط متوسط الشدة؛ حيث يكون متزامنًا مع استخدام الحرب التقليدية، وفي محاولة للتأثير النفسي والاقتصادي على الخصم في موازاة مع عمل الحرب التقليدي، وأما النمط الثالث من الصراع، فيطلق عليه نمط الحرب الساخنة، وهو يعكس حالة من التطور في استخدام الحرب الإلكترونية بدون تحريك الآلة العسكرية التقليدية، وهي ما تعبر عن حرب المستقبل. أما عن أهداف الصراعات الدولية السيبرية، فتدور حول المستوى الأول، التحكم في الفضاء الإلكتروني الدولي، والمستوى

(٤٢) Williamson, *Information Operations*: 15-22.

الثاني، حول تحويل القوة الافتراضية إلى مميزات استراتيجية، والمستوى الثالث، يتعلق بالصراعات الإلكترونية التي تهدد الأمن القومي للدول ذات السيادة.

١- الصراع الإلكتروني ونمط الحرب الباردة والمنخفض الشدة:

يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة، ويأتي هذا النمط ليعبر عن صراع ذي طبيعة ممتدة ومستمرة ودائمة النشاط العدائي أو غير السلمي، ويعبر هذا النمط عن صراعات أخرى أعمق وممتدة ذات نواحي ثقافية أو اقتصادية أو اجتماعية. ويتميز هذا النمط بدرجة كبيرة من التعقيد والتداخل في معركة لا نهاية لها، ما بقيت الأبعاد الأخرى للصراع، ولا يتطور هذا النوع من الصراعات بالضرورة إلى حالة استخدام القوة المسلحة بشكلها التقليدي أو من خلال شن حرب إلكترونية واسعة النطاق.

نمط «الحرب الباردة الإلكترونية» والتي أصبحت تمثل أكبر تهديد أمني لاستقرار العالم وأسواقه المالية وحتى للبنية التحتية المدنية من خلال شن الحرب النفسية والاختراقات المتعددة والتجسس وسرقة المعلومات وشن حرب الأفكار، ولا ترقى لعمل عسكري عنيف، ويأتي نمط الصراع الإلكتروني منخفض الشدة إلى عدة ملامح ومظاهر متعددة تتميز بالتنوع، وتعبر عن حالة الحراك الدولي بين الفرقاء والفاعلين في مجتمع المعلومات العالمي وعبر ظاهرة الفضاء الإلكتروني، وتتمدد من حالة الحرب الإعلامية والنفسية إلى حالات سرقة الأسرار الصناعية من خلال الاختراقات الإلكترونية والعمل السري أو من خلال انعكاس التنافس العالمي بين الشركات التكنولوجية عبر الفضاء الإلكتروني. وفي الصراع على المعلومات والنفوذ ما بين أجهزة الاستخبارات الدولية، ويقوم النشطاء بالقيام باختراق إلكتروني لنظم المعلومات والسيطرة، عبر استخدام الفيروسات أو هجمات إنكار الخدمة، وهو ما يتم في حالات الصراع السياسي ذي البعد الاجتماعي – الديني الممتد، مثل: حالة الصراع العربي الإسرائيلي أو الصراع ما بين الهند وباكستان أو ما بين كوريا الجنوبية والشمالية، والصراع ما بين مناطق الصراع التاريخية؛ حيث توجد اتجاهات العداء متبادلة يتم ترجمتها في شكل اختراقات إلكترونية أو من خلال توظيف القراصنة في شن



هجمات بهدف السرقة وتحقيق مكاسب مالية إلى جانب إمكانية توظيفهم لصالح جماعات أو أجهزة أمنية تابعة لدول بعينها.

وقد يأتي في إطار محاولة الدول المتقدمة اختبار دفاعاتها ضد الهجمات التي يُستخدم فيها الكمبيوتر سلاحًا دفاعيًّا، عن طريق اختراق أنظمة الكمبيوتر بهدف التأثير في محتواها أو سرقة معلومات أو تعطيل أدائها أو تدميرها، أو عبر شن الهجوم على الأقمار الصناعية الخاصة بالاتصالات أو محطات البثِّ أو كابلات الاتصالات. خاصة أن تحقيق السيطرة على الشبكات يمكِّن من السيطرة على الأسرار العسكرية والعلمية، بما يقود إلى أن تصبح حروب المستقبل باهظة التكاليف، وينشب الصراع من أجل تطوير القدرات في مجال أسلحة الفضاء الإلكتروني(٤٣).

وقد أثبتت حوادث الاعتداء التي قامت بها الجماعات الإرهابية أو حتى التي اتُّهمت بها الدول أنه ما زالت هناك حالة ضعف في دفاعات الدول وأمنها المعلوماتي أمام الهجمات الإلكترونية. وينشط دور جماعات دولية للقرصنة للتعبير عن مواقف سياسية مثل جماعة ويكيليكس وأنونيموس التي أصبحت تهدد شركات ودولاً بالاختراق، وكان منها قيامها بهجمات على مواقع حكومية. وقد تم استخدام الهجمات في الفضاء الإلكتروني في إطار الخلاف بين الدول فقد تم استخدامها في حالة الخلاف بين إستونيا وروسيا في عام ٢٠٠٧، وتعرضت المواقع الإلكترونية للتوقف والتدمير إثر شروع إستونيا في نقل تمثال من العهد السوفيتي يمثل الجندي المجهول الذي يعبر عن دور العرقية الروسية في مقاومة الغزو النازي. والاختراقات المتبادلة بين الصين والولايات المتحدة أو ما بين كوريا الجنوبية والشمالية أو ما بين إيران والولايات المتحدة(٤٤) أو باتهام إيران بشن هجمات إلكترونية على منشآت نفطية في الخليج العربي احتجاجًا على السياسات التمييزية ضد الشيعة.

(٤٣) Andy Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits", *Forbes* (23 Mar 2012), online e-article, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits.

(٤٤) David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012): 188; "Ralph Langner: Cracking Stuxnet, a 21st Century Cyber Weapon", *TED*, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.

٢- نمط الصراع الإلكتروني متوسط الشدة:

يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة، ويكون تعبيرًا عن حدَّة الصراع القائم بين الأطراف، وقد يكون مقدمة لعمل عسكري. وتدور حرب عبر الفضاء الإلكتروني عن طريق اختراق المواقع وقصفها وشنِّ حرب نفسية وغيرها. ويستمد ذلك الصراع سخونته من قوة أطرافه وارتباطه بعمل عسكري. وبخاصة مع تكلف فقط ٤٪ من تكلفة الآلة العسكرية، بما يمكِّن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابة. كما أنَّها لا تستغرق إلا وقتًا بسيطًا. ويتم استخدام الفضاء الإلكتروني في الصراع بطريقة موازية للحرب التقليدية.

وتاريخيًّا تم استخدامه في هجمات حلف الناتو عام ١٩٩٩ على يوغسلافيا، وتستهدف الهجمات شبكات الاتصالات ويعطلها، ما يؤدي تلقائيًّا لتوقف شبكات الجيش[٤٥]. وتم استخدام هذا النمط من الهجمات في الحرب بين حزب الله وإسرائيل في عام ٢٠٠٦، وتعرضت إستونيا إلى هجمات إلكترونية روسية عام ٢٠٠٧ على أثر الخلاف حول نقل تمثال يمجد دور الأقلية الروسية، وتم استخدام الهجمات الإلكترونية في حالة الحرب الجورجية – الروسية في أغسطس من العام ٢٠٠٨. وتم ذلك في المواجهات بين حماس وإسرائيل في عام ٢٠٠٩ وفي الحرب بين غزة وإسرائيل في نوفمبر ٢٠١٢. الصراع ما بين المعارضة السورية والنظام السوري عبر الفضاء الإلكتروني واستخدامه من قبل العديد من الحركات والتيارات المسلحة وبخاصة شبكات التواصل الاجتماعي، للحشد والتعبئة والتبرير وكمنصة للصراع فيما بينها أو مع غيرها. ولا تعكس بالضرورة قوة التجمعات الإلكترونية المختلفة على أرض الواقع بناءً على رصد أنشطتها على مواقع التواصل الاجتماعي.

٣- الفضاء الإلكتروني والصراع مرتفع الشدة:

ويتميز هذا النمط من الصراع على سيطرة البعد التكنولوجي على إدارة العمليات الحربية؛ حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، ويتم استخدام

(٤٥) Florian Bieber, "Cyberwar or Sideshow? The Internet and the Balkan Wars", *Current History* 99, no. 635 (Mar 2000): 124-128, online e-article, http://search.proquest.com/docview/200751259?accountid=7180.



الروبوتات الآلية في الحروب والتي يتم إدارتها عن بعد فضلاً عن الطائرات بدون طيار، ويتم تطوير القدرات في مجال الدفاع والهجوم الإلكتروني والاستحواذ على القوة الإلكترونية، ويتم استخدام الفضاء الإلكتروني في الاستعداد لحرب المستقبل والقيام بتدريبات على توجيه ضربة أولى لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية والبنية التحتية المعلوماتية. ولعل الهدف من وراء ذلك؛ تحقيق «الهيمنة الإلكترونية الواسعة» بشكل أسرع في حالة نشوب صراع.

ويتم التقدم في مجال استخدام كافة أنواع الأسلحة الإلكترونية مثل أسلحة الميكروويف عالية القدرة، وتم توجيه هجمات إلكترونية باستخدام عدد من الفيروسات مثل هجمات فيروس ستاكس نت في أكتوبر ٢٠١٠ ضد المنشآت النووية الإيرانية وفيروس دوكو وفيروس ستار في إبريل ٢٠١١، وفيروس فلام ودوكو ومهدي وجأوس وكان آخر الهجمات في ١٧ فبراير ٢٠١٢[٤٦]. بالإضافة إلى برمجيات تجسس مثل فينفيشر وركورا[٤٧]، وتبنت إسرائيل شن هجمات ستاكس نت بالتعاون مع الولايات المتحدة للعمل على تعطيل المنشآت النووية[٤٨]، ويمثل ذلك جزءًا من منصة لإطلاق الفيروسات الخطرة، تم تطويرها عام ٢٠٠٧. وتمت تجربته في إسرائيل[٤٩].

ويقدم النموذج الإيراني حالة فريدة لتحول الفضاء الإلكتروني لساحة قتال ذات طابع مرن وآخر ذو طابع صلب[٥٠]، وذلك في إطار المواجهة بين إيران وإسرائيل والولايات المتحدة، والتي منها استخدامه في تحريك القوة الناعمة داخل إيران بدعم الاحتجاجات في عام ٢٠٠٩، وتقديم دعم فني للمعارضة عقب الانتخابات الرئاسية، وفي نهاية ٢٠١١

---

(٤٦) "Iran Says Stuxnet Virus Infected 16,000 Computers", *Fox News: World*, http://www.foxnews.com/world/2012/02/18/iran-says-stuxnet-virus-infected-16000-computers/#ixzz1ntBzAB47.

(٤٧) Iran National CERT (MAHER), "Identification of a New Targeted Cyber-Attack", *Embeddedsw*, http://embeddedsw.net/doc/New_targeted_cyber-attack.html.

(٤٨) Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?" *PC World*, http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.

(٤٩) William. J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *The New York Times* (15 Jan 2011), online e-article, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&pagewanted=all.

(٥٠) عادل عبد الصادق، «الإنترنت والدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وإيران»، **مختارات إيرانية** (نوفمبر ٢٠١١).

دشنت الولايات المتحدة «سفارة إلكترونية» لتزويد الإيرانيين بالمعلومات حول التأشيرات عبر الإنترنت، والتواصل مع الطلاب الإيرانيين، وهو ما يلائم عملية قطع العلاقات الدبلوماسية بين إيران والولايات المتحدة منذ ثلاثين عامًا(٥١). وهو ما دفع إيران إلى حجب موقع السفارة وتجريم محاولة الدخول عليها على أنها تمثل تهديدًا للأمن القومي لديها(٥٢).

هذا إلى جانب التعرض إلى القوة الصلبة عبر الفضاء الإلكتروني عبر شن هجمات التخريب للبرنامج النووي للعمل على تعطيله وكانت آخر الهجمات في ١٧ فبراير ٢٠١٢ حين أعلنت الاستخبارات الإيرانية أن فيروس ستاكسنت أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر(٥٣). وذلك بعد أن تعرضت لهجوم ثالث عبر فيروس دوكو بعد فيروس ستاكس نت في أكتوبر ٢٠١٠ وفيروس ستار في إبريل ٢٠١١، وتبنت إسرائيل شن هجمات ستاكس نت بالتعاون مع الولايات المتحدة للعمل على تعطيل المنشآت النووية(٥٤) ويمثل ذلك جزء من منصة لإطلاق الفيروسات الخطرة، تم تطويرها عام ٢٠٠٧. وتمت تجربته في إسرائيل(٥٥).

ج- الفضاء الإلكتروني والحروب غير المتماثلة في العلاقات الدولية:

ظهر مفهوم «الحرب غير المتماثلة» Asymmetrical Warfare التي تعبر عن محاولة طرف يعادي الدولة القومية أن يلتفَّ من حول قوتها ويستغل نقاط ضعفها معتمدًا في ذلك على وسائل تختلف بطريقة كاملة عن نوع العمليات التي يمكن توقُّعها. وعدم التماثل يعني أن يستعمل العدو طاقة الحرب النفسية وما يصاحبها من شحنات الصدمة والعجز؛ كي ينتزع في يده زمام المبادرة وحرية الحركة والإرادة، وهو أسلوب يستخدم وسائل مستحدثة وتكنيكات غير تقليدية وأسلحة وتكنولوجيات جرى التوصل إليها وتطبيقها على كل مستويات الحرب

(٥١) "U.S. Launches 'Virtual' Embassy for Iran", *US Today News* (12 June 2011), online e-article, http://www.usatoday.com/news/washington/story/2011-12-06/us-embassy-iran/51673966/1.

(٥٢) J. David Goodman, "Iran Blocks American 'Virtual Embassy", *The New York Times* (7 Dec 2011), online e-article, http://thelede.blogs.nytimes.com/2011/12/07/iran-blocks-american-virtual-embassy.

(٥٣) "Iran Says Stuxnet Virus Infected 16,000 Computers".

(٥٤) McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?".

(٥٥) Broad, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay".

من الاستراتيجية إلى التخطيط إلى العمليات. ومن ثم فإن الحرب غير المتماثلة هي شكل غير تقليدي من الحرب؛ حيث يستخدم الطرفان أسلحة غير متماثلة، ويمتاز العدو بإرادة قوية وإصرار على تحقيق الأهداف(٥٦).

تُعَدُّ الحرب غير المتماثلة بمثابة مزيج من العلاقة ما بين التكنولوجيا والحرب، وهي نوع من الحروب يحاول أن يحُدَّ ويُقوّض من عناصر القوة لدى العدو وأن يستغلَّ نقاط ضعفه بطريقة مُبدعة جديدة تُحقق الانتصار الأخلاقي والمعنوي. وتكون معارك هذه الحرب في الجهة الخلفية للعدو، باستخدام العمليات الحربية النفسية ووسائل الإعلام، وعن طريق الإبداع الخلاق للقدرات المتوافرة والتشتت والاتصال وتلافي المعركة الفاصلة، من أجل شلِّ قدرات العدو وعزمه وإرادته. ويمثل نمط الحرب غير المتماثلة عودة إلى طُرق الحرب قبل ظهور وصعود مفهوم «الدولة»، وحيث تتحوّل عناصر القوة إلى ضعف وتُعاد صياغة معنى النصر والهزيمة. وتتحول بذلك طبيعة المعركة، وتصبح الأهداف: ضرب مراكز القوة الاجتماعية والاقتصادية والسياسية والثقافية، إضافة إلى العسكرية(٥٧).

تتميز الحروب الجديدة بأنها ذات أبعاد ثقافية وليست لأسباب جيوسياسية أو تنازُع حول السيادة الإقليمية بالضرورة. وتتميز كذلك باختلافها عن الحروب النظامية القديمة وحروب المناورات والجبهات وحروب العصابات. وأصبحت تلك الحروب الجديدة تتوخى الكسب السياسي للسكان عبر: كسب العقول والقلوب، زعزعة الاستقرار، زرع الخوف والحقد، السيطرة على السكان عبر إزالة كل هوية مختلفة. فهي حرب ضد الغريب وضد المخالف من داخل الجماعة نفسها. ويُعَدُّ طرد السكان والقتل الجماعي والتهجير القسري جزءًا من تقنيات الترهيب السياسي الجديد. وبات ضرب المدنيين والحصار والتعذيب والقتل الكيفي وتدمير المعالم الحضارية التاريخية والبنية التحتية من المباحات في تلك الحروب.

---

(٥٦) محمد عبد السلام، «الحرب غير المتماثلة بين الولايات المتحدة والقاعدة»، **مجلة السياسة الدولية**، العدد ١٤٧ (يناير ٢٠٠٢): ١٢٠.

(٥٧) David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, Cass Series: Strategy and History 9 (New York: Frank Cass, 2004): 269.

واعتمدت الحروب القديمة على تشكيلات عسكرية ذات تنظيم عمودي، أو قد تشمل وحدات منشقة عن الجيش وزعماء ميليشيات ومرتزقة ومافيات إجرامية واستخدام حتى جماعات إرهابية، وهي ذات تنظيم لا مركزي تنشط بمزيج من المواجهة والتعاون بين وحدات الجيش المختلفة عبر وسائل الاتصال الحديثة. وقد عملت الثورة التكنولوجية على إعادة التفكير في حركية وديناميكية الصراع. وظهر ما يُعرف بـ «عصر القوة النسبية» الذي يعني عجز القوة العسكرية عن تأمين الأهداف السياسية المترتبة عليها، مما يخلف آثارًا استراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي[٥٨].

تغيَّر «براديم» الحرب جذريًّا بانتقاله من نسق «الحروب الصناعية بين الدول» إلى نسق «الحرب في وسط الشعوب». ففي الحروب القديمة كان الغرض هو تدمير الخصم، إما باحتلال أرضه أو الاستيلاء على موارده. بينما أصبح الغرض في الحرب الجديدة هو التحكم في إرادته وخياراته. ومن ثم كان الدور المحوري للشعوب في هذا الصنف الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في البلد الذي يشنُّ الحرب، أو بالرأي العام الإقليمي والدولي. فأهداف الحرب هنا أصبحت أقل مادية، يؤدي فيها العامل النفسي والدعائي دورًا محوريًّا، سببه تنامي التغطية الإخبارية السمعية البصرية المباشرة للأحداث لحظة وقوعها.

إذا كانت الجيوش النظامية تسعى باستغلال تفوقها التقني العسكري – الإعلامي الكاسح لحسم حرب نظيفة سريعة تجنِّب السكان فظائع وآلام المواجهة، فإن استراتيجية الشبكات المسلحة المقاومة لها هي الاستخدام المعاكس لهذه الميزات التقنية، بالتسلل إلى وسط السكان والاحتماء بهم، وبالتالي تحويلهم إلى أرضية مواجهة، ومن ثم توجيه سلاح الصورة إلى مآسي الحرب وجرائمها الإنسانية.

في هذا المشهد تنمحي الفروق التقليدية بين الحرب والسلم، في الوقت الذي يغدو فيه الصدام السمة الغالبة على الوضع الاستراتيجي الدولي، وإن كان نادرًا ما يتطور إلى حالة مواجهة مسلحة؛ نظرًا للوعي المتزايد بعدم نجاعة الحسم العسكري في إطفاء بؤر التوتر

(٥٨) Lawrence T. Greenberg, Seymour E. Goodman and Kevin J. Soo Hoo, *Information Warfare and International Law* (Washington, DC: National Defense University Press, 1998): 20-34, online e-book, http://www.iwar.org.uk/law/resources/iwlaw/iwilindex.htm.



القائمة؛ والعلاقة غير المسبوقة القائمة بين التطرف ذي الخلفيات الدينية أو القومية وأسلحة الدمار الشامل الرخيصة وسهلة الإنتاج. وقد بدأت عملية إعادة التفكير في الردع القائم على التوازن السلبي المفضي إلى العجز والجمود. وظهر اتجاه للمزج بين عاملَي التنافس والتعاون، باللجوء إلى استراتيجية مواجهة متدرجة تؤدي إلى إنهاك الخصم للتغلب عليه. والذي أصبح غير ملائم للوضع الدولي مع بداية ظهور قوى صاعدة وظهور مشكلات عالمية تهم الأمن الإنساني المشترك.

أصبحت الحروب الجديدة نتاج ثورة في وسائل الاتصال وثورة المعلومات، وأيضًا ثورة في العلاقات الاجتماعية للحرب، واكتسبت الحروب الجديدة خصائصها كذلك من فراغ السلطة المميز للفترة الانتقالية التي ابتدأت بنهاية الحرب الباردة، وانهيار الأيديولوجيات وتفكُّك الوحدات السياسية ذات الطابع القومي، وانفتاح العالم على بعضه فيما عُرف بالعولمة التي عملت على تكثيف درجة التكامل والاعتمادية بين دول العالم، وزادت ثورة المعلومات من التفاعل والتجانس بالإضافة إلى تفتته وتنوعه. وبرزت هويات من داخل الدولة تريد التعبير عن مصالحها، مما زاد من حجم المطالب أمام الدولة، وأصبحت عاجزة في مواجهة تلك المطالب، فباتت عرضة للتمرد عليها وعلى احتكارها استخدام القوة المشروع.

جاء هذا التآكل لقوة الدولة من جانب السياق الدولي والمحلي، وضعفت قدرة الدولة على استخدام قواتها المسلحة انفراديًّا، وبات تنظيم القوات المسلحة متعددة القوميات، وبرزت ظاهرة خصخصة الأمن وشركات الأمن الخاصة التي يكون لها دور في الحروب (مثل شركة بلاك ووتر في العراق). ومع تآكل شرعية الدولة في مرحلة ما بعد الحرب الباردة، اندلع العنف الجديد المتمثل في ظهور الحرب الجديدة أو الفضاء الجديد مزيلاً الفروق بين المدنيين والمنشآت[٥٩].

(٥٩) John B. Sheldon, "Achieving Mutual Comprehension: Why Cyberpower Matters to Both Developed and Developing Countries", *Confronting Cyberconflict* 4, online e-article, http://marshall.org/wp-content/uploads/2013/12/Sheldon-Achieving-Mutual-Comprehension.pdf; Tom Gjelten, "Is All The Talk About Cyberwarfare Just Hype?", GBP News, http://www.gpb.org/news/2013/03/15/is-all-the-talk-about-cyberwarfare-just-hype.



كان اقتصاد الحرب القديمة يقوم على التنظيم المركزي الوطني للموارد، أما اقتصاد الحرب الجديدة فهو نقيض ذلك؛ بمعنى أنه ليس مركزيًّا تمامًا وإنما يعتمد على الموارد الخارجية وعلى التمويل الذاتي عبر الاعتماد على النهب والسلب، وأحيانًا السوق السوداء. ويعتمد هذا الاقتصاد على شبكات الضرائب وجذب مهاجري الشتات والمتاجرة بالسلاح وتهريب النفط، ويتم الحفاظ على هذه الموارد عبر قوة السلاح. ويعبر هذا الاقتصاد الحدود الدولية. وكانت استراتيجية المتحاربين تلتقي في هدف موحد هو زرع الخوف، ويتعاونون في خلق مناخ انعدام الأمن، وهناك حالات تعاون بين المتحاربين؛ تحقيقًا لمآرب عسكرية واقتصادية. وقد تهدف الحرب لدفع النمو الاقتصادي عبر تنشيط الصناعات العسكرية.

في الحرب التقليدية تكون هناك تحديات للقوة من حيث الكمّ والكيف، وتكون هناك حالة إعلان مسبقة للحرب[٦٠]. وتمثل الحرب غير التقليدية تحديًا لكون هجماتها استباقية، وتكون ساحة المعركة في الحرب التقليدية محددة زمانيًّا وجغرافيًّا وفي أطرافها، أما الحرب غير التقليدية فإنها غير محددة المجال أو المدى وتكون أهدافها غير مأمونة بخلاف الحرب التقليدية التي تكون أهدافها محددة كميًّا. وتكون القوات المستخدمة في الحرب التقليدية قوات نظامية، أما في غير التقليدية فتكون قواتها غير معروفة وليست محددة في دولة سواء أكانت هدفًا للحرب أم مشاركة فيها؛ ولا تصبح بالضرورة الدولة هي الهدف.

وتتميز الحرب التقليدية بأنها تشكل تحديًا عسكريًّا فقط، في حين تمثل الحرب غير التقليدية حربًا متعددة الأوجه ومتشابكة مع غيرها. ومن ثم تكون تفاعلاتها كبيرة بخلاف الحرب التقليدية التي تكون تفاعلاتها محدودة. وتصبح الحرب المعلوماتية متشابكة مع غيرها من الحروب الإعلامية وحرب الشبكات والاتصالات والحرب السياسية والسيكولوجية والحرب التكنولوجية والفضاء[٦١].

(٦٠) Kevin Coleman, "The Challenge of Unrestricted Warfare - A Look Back and a Look Ahead", *Directions Magazine*, http://www.directionsmag.com/entry/the-challenge-of-unrestricted-warfare-a-look-back-and-a-look-ahead/123237.

(٦١) المرجع السابق.

المبحث الثاني

الهيمنة السيبرانية والمزايا الاستراتيجية للأسلحة الإلكترونية

أولاً: الهيمنة الإلكترونية وإعادة تعريف القوة في العلاقات الدولية

على الرغم من احتفاظ دول كبرى بالهيمنة التكنولوجية في مجال الفضاء الإلكتروني والفضاء الخارجي، فإن إمكانية تحقيق التقدم أمام الدول الأخرى أصبحت متاحة، وبخاصة مع اعتماد ذلك التطور على التدريب والتعليم والقدرات البشرية المتوافرة، والتي تتميز بها الدول الأقل تقدمًا في مجال التكنولوجيا، وهو ما يجعل بعض الدول الكبرى تعمل على جذب العقول من العالم الثالث للعمل لديها ولخدمة مشروعها العلمي.

ساعد الفضاء الإلكتروني في تدعيم الهيمنة الإلكترونية، وتغيير الخريطة الإدراكية للدولة المستهدفة وتغيير رؤيتها لمصالحها الذاتية، وهو ما كان له تأثير على كيفية تأثير الفضاء الإلكتروني على استخدام القوة الإلكترونية عبر أدواتها المختلفة في الصراع الدولي، واستخدام القوة الناعمة عبر الدعاية وشن الحرب النفسية لممارسة الجذب وإقناع الآخرين وتقديم الإغراءات المالية والتدريب والثقافة بما يعزز من قدرات الدول في مجال توظيف الفضاء الإلكتروني في خدمة الأهداف الخارجية.

وهناك استخدام للهيمنة عبر القدرة على تطوير أسلحة إلكترونية متقدمة. وتمارس الولايات المتحدة هيمنتها المعلوماتية على العالم من خلال احتكارها للموارد الحرجة للفضاء الإلكتروني أو من خلال سيطرتها التكنولوجية، سواء عبر الفضاء أو أقمار الاتصالات والتجسس، وهو ما أضاف لقوة الولايات المتحدة قوة أكبر على الهيمنة وممارستها عبر تأثيرها المباشر والعميق في شعوب العالم عبر دعم حرية الإنترنت وحقوق الإنسان.

وأصبحت الهيكلية العالمية ترتبط بمعدلات توظيف الفضاء الإلكتروني في الاقتصاد العالمي وتحريك الاستثمار والتجارة بين الدول، وهو ما جعل القوة الاقتصادية الجديدة تفوق في أهميتها القوة العسكرية على المسرح العالمي. وانتهاك سيادة الدول النامية وإلى

إيجاد شكل جديد من التبعية التكنولوجية إما بسبب تقدم الدول الكبرى أو خضوعها لسيطرة الشركات المتعددة الجنسيات. وأصبح هناك فجوة رقمية بين الجنوب والشمال في مجال القدرات المعرفية والتكنولوجية(٦٢).

وحلت الهيمنة الإلكترونية محل الأشكال الأخرى التقليدية، وأصبح لها أبعاد مختلفة كدورها الثقافي بنقل القيم الغربية إلى العالم في مواجهة القيم المحلية. وفيما يتعلق بحجم التدفق الدولي للمعلومات، والتي إلى جانب تأثيرها الاقتصادي يوجد تأثير معنوي يتعلق بالقدرة على احتلال العقول، وهو أخطر بكثير من احتلال الأرض، من خلال اختراق المجتمعات وتقوية روافد داخلية لها ارتباطات متحالفة أو متعاطفة مع قوى خارجية.

وأتاح الفضاء الإلكتروني آليات جديدة للهيمنة، وذلك عبر فرض الهيمنة الاقتصادية والثقافية والعسكرية والاجتماعية عبر القدرة على احتكار عمليات تدفق المعلومات والاستحواذ على القوة الإلكترونية الصلبة والناعمة في تمدد النفوذ الخارجي، وهو ما خلق نظامًا إعلاميًّا دوليًّا عالميًّا يسيطر على عملية تنظيم تدفق البيانات عبر الحدود، والتحكم فيها وتحديد سياسة الدولة في المجالات الاقتصادية والثقافية، وهو الأمر الذي جعل العالم الثالث يخضع لشكل جديد من التبعية عبر التأثير على دوله من الخارج عبر تدفق المعلومات المنتجة من قوى خارجية إليها، أو عبر استيرادها للتكنولوجيا، وبما يجعلها تحت عملية تخطي الحدود المعلوماتي للحدود القومية، عبر ضح المنتجات الثقافية إلى داخل الدول بما يؤثر على القيم المحلية.

وعلى مستوى عملية إنتاج وتدفق المعلومات جاء الفضاء الإلكتروني ليحكم الهيمنة الغربية على العالم، وليضاف إلى السيطرة على مجال الإنتاج الإعلامي، فلا تزال وكالات الأنباء الغربية الأربع الرئيسية وهي رويترز ووكالة الصحافة الفرنسية AFP والآسوشيتد برس AP واليونايتد برس إنترناشيونال UPI تتحكم في توزيع ما يقرب من ٩٠٪ من الأخبار في العالم. وتسيطر الولايات المتحدة الأمريكية وحدها على ما نسبته ٤٠٪ من الإنتاج التلفزيوني والسينمائي في السوق العالمية. وتحتكر ثلاث أو أربع وكالات غربية إنتاج

(٦٢) خالد محمد غازي، **الطوفان: العولمة: فك الثوابت وتحطيم الهويات** (القاهرة: دار الهدي، ١٩٩٨).



وتوزيع الأخبار التليفزيونية المصورة منها وكالة فيز نيوز ووكالة روتير البريطانيان ووكالة اليونايتد برس المصورة الأمريكية ووكالة الـدي.بي.إيه DPA الألمانية. ويضاف إليها شبكة سي.إن.إن CNN والشبكة الكابلية الإخبارية Cable News Network والشبكة الأمريكية ورلد نت World Net، وتعد الولايات المتحدة الأمريكية هي القوة الأولى المصدّرة للثورة التقنية الإلكترونية، إذ تتحكم بنسبة ٦٥٪ من مجمل الاتصالات الدولية.

أثر الفضاء الإلكتروني على الهيمنة على المستوى الدولي، وأثر على محدداتها والفاعلين في الهيمنة وانتقالها من الدول إلى الشركات التكنولوجية الكبرى، والتي ما هي إلا غطاء لدول كبرى تحركها وفق مصالحها، وعكس الفضاء الإلكتروني حالة من عدم التوازن في تدفق المعلومات والأخبار بين الدول المتقدمة والنامية؛ وذلك في سبيل السعي إلى إيجاد نظام دولي للاتصالات يلائم التطورات التي فرضها تطور ظاهرة الفضاء الإلكتروني، والتي فرضت أطرًا للتعاون، وفي نفس الوقت أتاحت الفرصة لتعزيز الهيمنة والسيطرة فيما يعرف «بنظرية الاستقرار الهيمني» والتي كان من روادها كابلان. وهو ما قد ينصرف إلى أن تأثير الفضاء الإلكتروني في بنية النظام الدولي من شأنه أن يحدث إما تعظيمًا للقوة المهيمنة على النظام الدولي أو بروز قوى جديدة، وهو ما يعيد التفكير في القوة.

وقدمت حنا أرندت ترتيبًا لمستويات القوة، وعني الأول باستخدام العنف والقهر، والذي يمكن مراقبته وهو يأتي في شكل حروب وعمليات عسكرية على أرض الواقع، أما المستوى الثاني فيختص بالتحكم في البدائل المتاحة والتحكم في جدول الأعمال، والمستوى الثالث هو أعلى مراحل القوة، وهو ما يعني استخدام بعض عناصر القوة الأساسية بشكل يؤثر على طبيعة الصراع على القوة.

وإن كانت الهيمنة قد ارتبطت في الماضي بالسيطرة على الاقتصاد المعتمد على الموارد الطبيعية وحجم الجيوش، فإن الهيمنة في عصر الفضاء الإلكتروني قد ارتبطت بالقدرة على التحكم والسيطرة في التكنولوجيا والقدرة على ممارستها ليس فقط على الدول أو على الأرض بل باتساعها مع تمدد الفضاء الإلكتروني، وتجاوز الحدود وسيادة الدول؛ وهو ما



مكن الدول الكبرى في ممارسة أشكال متعددة من الهيمنة منها الجانب الثقافي والاقتصادي والعسكري والتكنولوجي.

وإن كان العالم قد شهد قديمًا الاستعمار والذي كان يرتكز على توسع من جانب الدول القوية لحساب دول أخرى تقوم باحتلالها وإخضاعها بالقوة بهدف نهب ثرواتها الطبيعية وتسخير طاقاتها البشرية في خدمة مصالحها. وتقوم الدول الاستعمارية القوية باحتلال أراضي الدول الضعيفة وإخضاع شعوبها بقوة السلاح. فإن الفضاء الإلكتروني قد عمل على تغيير المعادلة وأطرافها ومساراتها وقوة الفاعلين في ممارسة الهيمنة. وعزز الفضاء الإلكتروني من فرص ممارسة الهيمنة السيبرانية Cyber-Hegemony[٦٣].

تتعلق «الهيمنة الإلكترونية» بُبعد صلب ترتبط بالقدرة على امتلاك مقدرات وأسلحة الاستحواذ على الفضاء الإلكتروني، إلى جانب القدرة على التأثير المعنوي والنفسي في قطاعات عريضة من الجماهير، والتي تؤدي إلى تعميق التبعية للخارج. وساعد على ذلك تعدد استخدامات الفضاء الإلكتروني في مجال الثروة والمعرفة. والتي أدت إلى بروز التبعية الاقتصادية والتغريب والتنميط الثقافي. عبر إنتاجها الاحتكاري لأدوات الهيمنة.

وقد أثارت عملية انتشار القدرات التكنولوجية في النظام الدولي إلى التأثير كذلك على نمط انتشار القوة في النظام العالمي، والتأثير على قدرات الدول المهيمنة مثل الولايات المتحدة، والتي على الرغم من احتكارها للقدرات العسكرية التقليدية وغير التقليدية فإنها أصبحت في مرمى التهديد والخطر من جانب دول أخرى نتيجة قدرتها على اختراق نظمها الدفاعية عبر شبكات الاتصال والمعلومات، ومن ثم فإن القدرات الفعلية التي تمتلكها الولايات المتحدة لم تتواكب مع مكانتها العالمية، وإلى الحد الذي يمكن القول إن ذلك مثل نهاية مفهوم القوة العظمي[٦٤].

(٦٣) William Dan Perdue, "The New Totalitarianism: Cyber-Hegemony and the Global System", *International Progress Organization*, http://i-p-o.org/perdue.htm.

(٦٤) Ted Galen Carpenter, "The New World Disorder", *Foreign Policy*, no. 84 (1991): 24-39.

وأصبحت الحروب السيبرانية – الإلكترونية تعمل على تقويض النظام العالمي القائم، وبخاصة في حالة تحولها إلى اشتباكات عسكرية بين البلدان(٦٥)، وسعت العديد من الدول إلى إنشاء وحدات داخل الجيوش الحديثة تختص بالمجال الإلكتروني. وترى الصين أن الأنظمة الدولية ذات الصلة يجب أن تتم في إطار الأمم المتحدة وأن بكين قدمت اقتراحات محددة(٦٦).

ثانيًا: خصائص الأسلحة والهجمات الإلكترونية

من التعريفات الشائعة للأسلحة هي «أي أداة أو وسيلة تستخدم في القتال»، أو أي وسائل يتم توظيفها للتفوق على الآخرين، ويتم توجيه الأسلحة الإلكترونية إلى الهجوم على الأنظمة المرتبطة بالفضاء الإلكتروني لدولة أو خصم آخر، وتستخدم الأسلحة الإلكترونية كأسلحة غير مرئية ولديها القدرة على التدمير الشامل بدون تهديد حقيقي للبنية التحتية الحيوية أو حياة الإنسان بالضرورة مع إمكانية حدوث ذلك(٦٧).

فعرّف كل من ريتشارك كلارك وروبرت كناكي الحرب الإكترونية على أنها «أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها. فيما يعرّف آخرون مصطلح الحرب الإلكترونية بأنها «مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي»(٦٨).

وتتكون البنية التحتية لتطوير قدرات الأسلحة الإلكترونية من جهاز كمبيوتر، أو هاتف محمول متصل بالإنترنت وسلسلة من برمجيات تقليدية، وبرمجيات خبيثة وبرامج تجسس

---

(٦٥) "Cyber Warfare Subject to Western Hegemony", *Global Times*, http://www.globaltimes.cn/content/770576.shtml#.Ugao-KxlfFw.

(٦٦) Sutirtho Patranobis, "China Doesn't Want Cyberspace Hegemony", *Hindustan Times*: *Beijing* (June 2013), online e-article, http://www.hindustantimes.com/world/china-doesn-t-want-cyberspace-hegemony/story-4rRyFbxLNhnpO2X9lod0BL.html.

(٦٧) Guy-Philippe Goldstein, *Cyberspace and National Security: Selected Articles*, edited by Gabi Siboni (Isreal: The Institute for National Security Studies, 2013), online e-book, http://www.inss.org.il/uploadImages/systemFiles/CyberENG3925062787.pdf.

(٦٨) علي حسين باكير، «المجال الخامس.. الحروب الإلكترونية في القرن الواحد والعشرين»، **مركز الجزيرة للدراسات: قضايا** (١٢ يناير ٢٠١١)، http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html.

وما إلى ذلك. ولا تحتاج عملية التطوير لمعدات متخصصة أو يمكن حظرها، كما يتم في حال الأسلحة النووية والتي تحتاج عمليات تخصيب اليورانيوم وخدمات لوجستية معقدة، وموارد مالية هائلة. وتحتاج الأسلحة النووية لإطلاقها إلى التطور في مجال الصواريخ الناقلة لها والعابرة للحدود.

بينما تتطلب الأسلحة الإلكترونية مهارات نادرة لإنتاجها ولا تحتاج تلك الأسلحة لإطلاقها سوى منصات بسيطة وغير مرئية تتمثل موقع إطلاق وكمبيوتر ثابت أو محمول، هاتف محمول، موقع على شبكة الإنترنت، محرك للبحث، شبكة اجتماعية، خادم افتراضي أو مادي أو «سحابة بيانات»، تشكل جميعها منصات الإطلاق. ويمكن تصميم واستخدام الأسلحة الإلكترونية من أي مكان، من قبل أي شخص، مثل القراصنة، المتطرفين الدينيين أو السياسيين، المجرمين الإلكترونيين، موظف سابق ساخط على شركته، منافسين، دول متصارعة، ولا تترك الأسلحة الإلكترونية سوى القليل من الوقت للاستباق والوقاية والكشف أو رد الفعل بسبب السرعة الإلكترونية للهجوم.

وتتيح البيئة الإلكترونية الاستراتيجية والمتعددة الحدود ولسيادة الدول، عملية استخدام الأسلحة الإلكترونية لاختراق نظم العدو بغرض التجسس أو الحرب النفسية أو الردع أو تدمير نظم المعلومات أو أهداف طبيعية، وأصبحت الحرب الإلكترونية إحدى الطرق الدفاعية التي تستخدم من قبل الدول لحماية مصالحها من الدول المعادية، وأصبح هذا الاتجاه يشهد تسارعًا في العلاقات الدولية. وسمح الفضاء الإلكتروني للدول التي لديها موارد وقدرات تكنولوجية عالية في توظيفها في إنشاء وتطوير ترسانتها من الأسلحة الإلكترونية لشن الهجمات الإلكترونية، والدول الضعيفة تكنولوجيًا يمكن أن تشكل تهديدًا بتطوير أسلحة إلكترونية هجومية[٦٩].

وتستخدم الأسلحة الإلكترونية للحصول على المبادأة في ميدان المعركة بوحدات كمبيوترية كالوحدات الأساسية في القوات المسلحة، وذلك بالاستخدام الصحيح

(٦٩) Daniel Cohen and Aviv Rotbart, “The Proliferation of Weapons in Cyberspace”, *Military and Strategic Affairs* 5, no. 1 (May 2013): 59-61, online e-article,
http://www.inss.org.il/uploadImages/systemFiles/MASA5-1Eng4_Cohen%20and%20Rotbart.pdf.

والمتقن لجميع الأسلحة المعلوماتية عبر صراع إلكتروني بين القيادات الصديقة والقيادات المعادية بهدف التأثير على قدرات الخصم واختراق كيانه الإلكتروني. والتي قد تأتي عبر شن الضربات الاستباقية لمواجهة تهديد محتمل؛ والحروب بالوساطة كأن تبيع إحدى المنظمات المتخصصة في الأعمال العسكرية خدماتها المعلوماتية والأمنية إلى بعض الجهات؛ والحروب «السرية» التي تتخذ طابعًا خاصًّا في الفضاء الإلكتروني لأنها تعتمد على أنواع متطورة من الفيروسات الإلكترونية، إضافة إلى هجمات «الهاكرز» المُنسّقة ومعارك المنافسة بين شركات برامج حماية الكمبيوتر وصُناع الفيروسات المعلوماتية.

وعلى الرغم من الاستخدام الواسع في وسائل الإعلام لمسمى «الحرب الإلكترونية»[٧٠]، فإنه لم يعد كافيًا إثر اتساع مدلولاته بعد أن كان مقصورًا في التشويش على أنظمة الاتصال والـرادار وأجهزة الإنـذار، بينما يكشف الواقع الحالي عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات الحربية، أما إطلاق مسمى «الحرب» على هجمات الكمبيوتر، فهو أيضًا بحاجة إلى إعادة النظر حيث يركز «الحرب» على استخدام الجيوش النظامية، وكان يسبقها إعلان مسبق واضح لحالة الحرب وميدان قتال محدد.

وتتحرك الأسلحة الإلكترونية عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية، والتي يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق العملاء لأجهزة الاستخبارات، والتي تتميز بهجمات الكر والفر واستحواذ الخوف والرعب، وبشكل جعل عملية استخدام هجمات الكمبيوتر سياسيًّا في أي صراع أقرب إلى توصيفها بالإرهاب عن كونها حربًا، ولا يحمل ذلك تقييمًا أخلاقيًّا لها بقدر ما هو تعبير عن طبيعتها الفنية وطرق حدوثها[٧١]. ويمكن أن تقوم القوات الخاصة لأي دولة بشن هجمات باستخدام الأسلحة الإلكترونية في مهاجمة البنية التحتية المعلوماتية الخاصة بدولة أخرى[٧٢]. وتتميز عملية

(٧٠) يوجد عدد كبير من المسميات باللغة الإنجليزية التي تحاول أن تصف ذلك النشاط، والتي منها:
Cyber war, Net war, Computer network attacks, Information warfare, Cyberterrorism, Electronic war, Asymmetric war, Cyber-attacks.

(٧١) عادل عبد الصادق، **الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة** (القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية، ٢٠٠٩): ١٥٥–٢٢٩.

(٧٢) Mark R. Shulman, "Discrimination in the Laws of Information Warfare", *The Columbia Journal of Transnational Law 37*, no. 3 (1999): 937- 998.

استخدام الأسلحة عبر الفضاء الإلكتروني بسهولة الانتشار والقدرة على التأثير على الأهداف «الجاهزة إلكترونيًّا» كالبنية التحتية الحيوية والمؤسسات الاقتصادية والمالية والسياسية والعسكرية[٧٣].

وبرزت ترسانة غير تقليدية لأسلحة إلكترونية Cyberweapons[٧٤] تتمتع في استخدامها بمزايا استراتيجية، يمكن صنع ترسانة إلكترونية بقدر تكلفة دبابة، بالإضافة إلى أن مصدرها يمكن أن يبقى مجهولاً ويمكن إنجاز الهجوم في زمن قياسي، وتعتمد على الترويع وبث الخوف، ولا يمكن معرفة الحجم الفعلي للخسائر، ولا بمعرفة الكيفية التي تم بها الهجوم.

وتدخل هجمات الأسلحة الإلكترونية في إطار الحروب غير المتكافئة War Asymmetric كون الطرف الذي يتمتع بقوة هجومية ويبادر باستخدامها هو الطرف الأقوى، بغض النظر عن حجم قدراته العسكرية التقليدية، وصعوبة التمييز في إطار الحرب الإلكترونية بين ما هو منشآت مدنية والأخرى ذات الطبيعة العسكرية، ولا تتطلب لتنفيذها سوى وقت زمني محدود. وتلعب المهارات البشرية دورًا أساسيًّا في تطويرها. ويعد استخدام الأسلحة الإلكترونية جزءًا من عمليات المعلومات المستخدمة في مستويات ومراحل الصراع المختلفة على الجانب التكتيكي أو الاستراتيجي أو العملياتي ويتم ذلك بطرق عديدة[٧٥].

وتشن تلك الهجمات السيبرانية من خلال الجيش والمجتمع بما يمثل أسلوبًا عسكريًّا غير نمطي لإدارة الصراعات المسلحة من خلال اشتراك منظمات غير حكومية وأفراد مدنيين عبر الفضاء الإلكتروني، وصعوبة تحديد مواقع المتحاربين في ميدان الحرب، ويصبح القطاع المدني المشترك في الحرب واسع وضخم ومن المستحيل تحديد حجمه وأبعاده، ويصبح المبرمجون والهواة والمتعاطفون مع مواقف الدول أو الجماعات الإرهابية بإمكانهم

---

(٧٣) Libicki, *Conquest in Cyberspace:* 13-323.

(٧٤) John Markoff, "Vast Spy System Loots Computers in 103 Countries", *The New York Times* (28 Mar 2009), online e-article, http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=2&hpw.

(٧٥) متعددة كالفيروسات وهجمات إنكار الخدمة والاختراق وسرقة المعلومات والتشويش. وتتميز هجمات الفضاء الإلكتروني بالحداثة والتنوع كقطع كابلات الإنترنت، ونشر الفيروسات، وهجمات إنكار الخدمة، والاختراق، وسرقة المعلومات، والتشويش. وهناك ما يعرف بالقنابل الإلكترونية، والتي تستهدف تعطيل الاتصالات والتشويش عليها، والتنصت على المكالمات، وبث معلومات مضللة عبر شبكات الحاسب والهاتف، واستهداف شبكات الحاسب بالتخريب عن طريق نشر الفيروسات، ومسح الذاكرة الخاصة بالأجهزة المعادية. وهناك أسلحة خاصة تعتمد على الطاقة الموجهة، ومنها أسلحة الميكروويف عالية القدرة، وتعزيز الأنشطة الاستخباراتية في الدول الأخرى.



إدارة الحرب من أجل تحقيق النصر والدفاع، ويتطلب أن يكون الجنود مؤهلين علميًّا وتقنيًّا لاستخدام أسلحة متطورة تكنولوجيًّا.

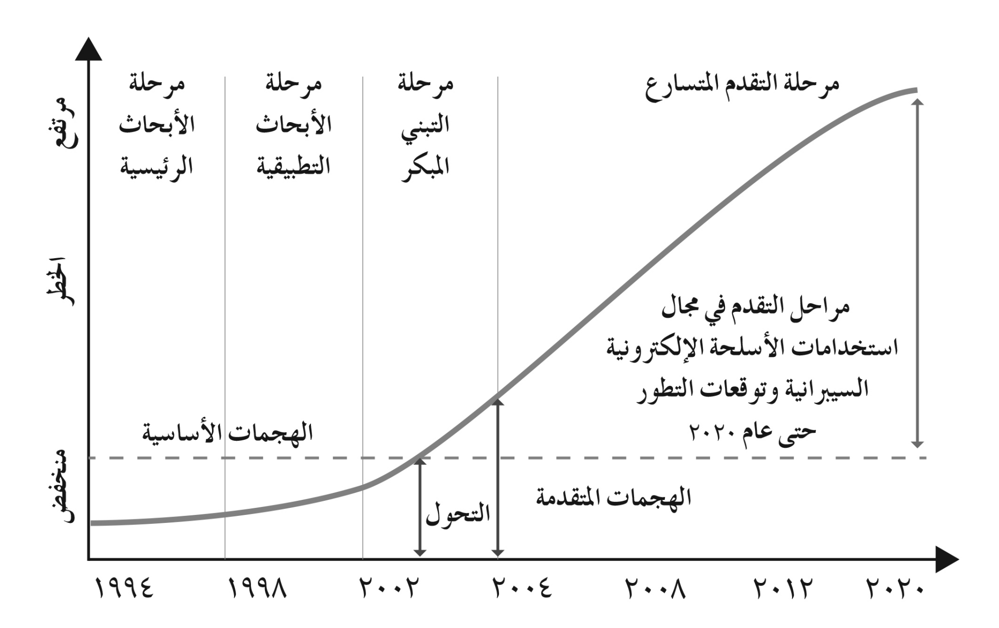
وقد تقوم دولة باستخدام هجمات الفضاء الإلكتروني كجزء من الاستعداد لنشوب صراع وحرب وهجوم تقليدي ضد دولة معادية، وخاصة أن هجمات الفضاء الإلكتروني استباقية من دون سابق إنذار، وأنها غير محددة المجال أو المدى وتكون أهدافها غير مأمونة بخلاف الحرب التقليدية التي تكون أهدافها محددة ومكانها محددًا، وتكون قوات الحرب الإلكترونية غير معروفة وليست محددة في دولة سواء أكانت هدفًا للحرب أو مشاركة فيها، لا تصبح بالضرورة الدولة هي الهدف، وتكون الحرب الإلكترونية متعددة الأوجه ومتشابكة مع غيرها، ومن ثم تكون تفاعلاتها كبيرة، فهي تتشابك مع الحرب الإعلامية وحرب الشبكات والاتصالات والحرب السياسية والسيكولوجية والحرب التكنولوجية والفضاء[٧٦].

وتصبح الدولة ضحية إذا ما تم مهاجمة نظم شبكاتها الإلكترونية وتأثير هذا الهجوم «تخريبي» على البنية التحتية للمنشآت الحيوية، مثل منشآت الطاقة والكهرباء والمؤسسات المالية والمصرفية وغيرها، وبدون معرفة من وراء الهجوم وكيفية نجاحه وطرق تنفيذه وأطرافه الحقيقية، مما يجعله قضية متشابكة، وتأتي عملية الاستجابة للهجمات وعملية رد الفعل مع ضعف إجراءات الوقاية ضد التعرض لمثل تلك الهجمات، والتي يمكن أن يتم شنها عبر الفضاء الإلكتروني والشبكات، أو من خلال استخدام الهجوم العسكري التقليدي، وللحصول على تأييد دولي للإجراءات الوقائية السلبية تكون هناك حاجة ملحة إلى تقديم الدليل أو إثبات تورط طرف ما في مثل هذا الهجوم – والذي يكون من الصعب التأكد بشأنه – بما يشكل ضمانة لوجود إجماع دولي للتعاون في المكافحة أو الحرب ضد طرف آخر أو فرض عقوبات دولية ما، حيث تكون الدول معرضة لانتهاك لسيادتها وأمنها الداخلي[٧٧]. ومن ثم فإن الدولة الضحية يتم إصابتها دون النظر إلى حدودها أو نطاقها الجغرافي ولا يلقى هذا النمط الجديد من الصراع تنديدًا دوليًّا مثل الهجوم التقليدي.

(٧٦) Coleman, "The Challenge of Unrestricted Warfare - A Look Back and a Look Ahead".

(٧٧) Bonnie N. Adkins, *The Spectrum of Cyber Conflict from Hacking to Information Warfare: What Is Law Enforcement's Role?* (Alabama: Air University. Air Command and Staff College, 2001): 78-89.

وتشير توقعات تطور استخدام الأسلحة الإلكترونية حتى عام ٢٠٢٠، حيث تنتقل من مراحل الهجمات الأساسية في الفترة من ١٩٩٤–٢٠٠٢، ثم تدخل مرحلة التحول ما بين عامي ٢٠٠٢–٢٠٠٤، وتدخل بعد ذلك في مرحلة الهجمات المتقدمة من ٢٠٠٤–٢٠٢٠[٧٨].



ثالثًا: المزايا الاستراتيجية للتوظيف العسكري للأسلحة الإلكترونية

تتميز عملية استخدام الأسلحة الإلكترونية – السيبرانية بعدد من المزايا الاستراتيجية، والتي تشكل حافزًا للعمل على امتلاكها وتطويرها واستخدامها، وأهم تلك المزايا هي:

- تتمكن الأسلحة الإلكترونية من تجاوز القيود الجغرافية، وتنفيذ الهجمات ذات مدى طويل وبسرعة البرق، دون الاحتكاك بالخصم في المجالات المادية. ويفرض قدرة

(٧٨) Kevin G. Coleman. “Cyber Intelligence: Cyber Arms Race Is Well Underway”, *Breaking Government* (9 Sep 2011), online e-article, http://breakinggov.com/2011/09/09/cyber-intelligence-blog-cyber-arms-race-is-well-underway.

الهجوم السريعة الاعتماد على أنظمة حماية ديناميكية ولديها درجات استجابة سريعة في الوقت الحاسم.

• قدرة العمل السرية

يتم تطوير الأسلحة الإلكترونية دون أن يتم اكتشافها مع القدرة على الاختفاء ونسج هالة من الغموض حول الجهود التسليحية على مستوى البحث والتطوير وتنمية القدرات الهجومية والدفاعية، وهو ما يحمل تحديًا حول إمكانية السيطرة على تلك الأسلحة بعكس الأسلحة التقليدية الأخرى.

• سلاح غير قاتل وغير مرئي

يمكن للأسلحة الإلكترونية أن تنفذ أهداف الهجوم دون إلحاق ضرر مادي بالبنية التحتية أو بالبشر، وهو ما يعد ميزة تختلف عن استخدام الأسلحة التقليدية الأخرى، ويمكن بواسطة هجمات الفضاء الإلكتروني أيضًا إحداث دمار بالغ بالبشر عن طريق ضرب الأنظمة المتصلة بمجال الفضاء الإلكتروني والموجودة في المجالات المادية.

• إصابة أهداف استراتيجية يصعب الوصول لها عبر هجوم تقليدي مثل:

أ- المنشآت والأنظمة المتواجدة في مناطق من الصعب مهاجمتها بالنيران نظرًا للبعد الجغرافي والحماية النيرانية القوية، ووجود تجمعات سكانية وغير ذلك.

ب- الفروع البنكية والمالية وهي بنى وطنية حساسة مُعرضة لهجوم الفضاء الإلكتروني سواء بسبب ارتباط الدول الكبير بالنظم المالية، أو بسبب ارتباط تلك النظم بمجال الفضاء الإلكتروني.

ج- أنظمة لوجستية ومواصلات، وتعتبر اليوم محوسَبة.

د- قواعد بيانات الدولة - وزارات الحكومة وهيئة القضاء وجامعات وغيرها.

- خطر ضئيل على حياة الإنسان

يكمن في الهجوم باستخدام الفضاء الإلكتروني خطر ضئيل على حياة المُهاجِم مقابل الهجوم العسكري النيراني، والذي فيه تعرض القوات للخطر، وهو أحد الاعتبارات التي قد تمنع الهجوم. هذا الأمر صحيح على الصعيد الدفاعي، حيث توفر هذه الخاصيّة للجانب المدافع حرية عمل كبيرة وكافية وكذلك قدرة تشغيل وسائل أوتوماتيكية ضد الهجوم، دون تفكير بشري ودون تعرض حياة الإنسان للمخاطر. سواء على صعيد المهاجم أو على صعيد المدافع. وهذا على عكس منظومات الدفاع النيرانية. فعلى صعيد المهاجم، توفر كثير من الجراءة لدفع أفكار هجومية.

- الانتقائية مقابل العشوائية

هذه الميزة ليست واضحة، ففي تصوّرات هجومية معيّنة يمكن مهاجمة أهداف مكتظة داخل مجال مُعيّن دون الإضرار بكيانات أخرى. ومع ذلك، في تصوّرات هجومية أخرى من الصعب التحكم في أبعاد الهجوم، ورُبّما يتمدد الهجوم لما وراء ما هو مخطط له.

- الطابع الانتشاري للأسلحة الفيروسية

هذه الخاصيّة تتصل باتجاه الفيروسات لاستنساخ نفسها دون توقف وقدرتها على التحرك داخل الشبكة في أماكن مختلفة، وهذه الخاصيّة تعتبر تحديًا صعبًا للطرف المدافع، الذي عليه منع استشراء الفيروسات لأماكن مختلفة. وأفضلية للمُهاجِم في تصوّرات معيّنة لهجوم عريض. فبواسطة جهد محدود يمكنه إيجاد تأثيرات كثيرة. وهذه الخاصيّة قد تُمثّل صعوبة للمُهاجِم الذي يبدي اهتمامًا بتصوّرات هجومية مُركزة وانتقائية ورقابة على نتائج الهجوم.

- الطابع المعياري العالمي لمجال الفضاء الإلكتروني

يعتمد الفضاء الإلكتروني على وجود تطبيقات موحدة ويتم تطويرها من قبل شركات تكنولوجية عالمية، والتي تعمل في جميع الدول وتتصل ببعضها، وهو ما قد يشكل خطرًا

إذا ما تم اختراق تلك الأنظمة وبرامج أمن المعلومات، وهو ما من شأنه أن يمثل خطرًا على كل الأمكنة التي تستخدمه.

- رخص تكلفة الإنتاج

بمقدور دول تشكيل قوات للفضاء الإلكتروني ذات قدرات هجومية متقدمة بتكاليف زهيدة في مقابل تلك الراغبة في بناء قوات نيرانية متقدمة، وكذلك بمقدرة منظمات وجماعات أن تتسلح وتُشغّل سلاح الفضاء الإلكتروني. وجميعهم يمكنه استئجار مواطنين وشركات خاصة كي تعمل لصالحهم. وتزيد القدرة على التعبئة في حالة القتال عبر استخدام الفضاء الإلكتروني، وهو ما يعمل على تقليل تكلفة التعبئة القتالية.

- قدرة تحكم بشرية عالية في الفضاء الإلكتروني

نظرًا لكون مجال الفضاء الإلكتروني مجال صناعيّ، ومُنتج بشري، وهو ما يساعد إلى درجة كبيرة في التحكم والسيطرة على بيئة ومناخ القتال مقارنة بالمجال البري، والذي يمكن أن يكون الطقس عائقًا يؤثر على سير الأعمال القتالية ويوفر الفضاء الإلكتروني بيئة مستقرة إلى حد ما مع تلافي الأخطاء البشرية وتهديد العناصر الداخلية، والتي يمكن للأطراف المهاجمة أو المدافعة أن تقوم بخضوعه للتدريب وإجراء المناورات.

- الفضاء الإلكتروني مجال مدني – عسكري مشترك

في كثير من الحالات تكون البنى التحتية العسكرية للاتصالات مرتبطة بالبنى التحتية المدنية للاتصالات، وهو ما يجعل الدفاع عن البنى المدنية حيويًا للأغراض العسكرية. والذي يمكن أن يتم عبر استخدام الجيوش لقدراتها في مجال الفضاء الإلكتروني، وهو ما قد يواجهه بصعوبات تتعلق بعملية جمع المعلومات وتشغيل الوحدات العسكرية في الفضاء الإلكتروني المدني.



• اعتمادات متبادلة بين مجال الفضاء الإلكتروني والمجالات المادية

يعتمد مجال الفضاء الإلكتروني اعتمادًا ذا اتجاهين مع المجالات المادية: من ناحية، تعاظم العمليات في تلك المجالات، ومن ناحية ثانية يعرض البنية التحتية الموجودة في تلك المجالات للخطر مثل الكابلات البحرية والمرافق الحيوية ومحطات الاتصالات.

رابعًا: تصاعد القدرات في سباق التسلح السيبراني عبر الفضاء الإلكتروني

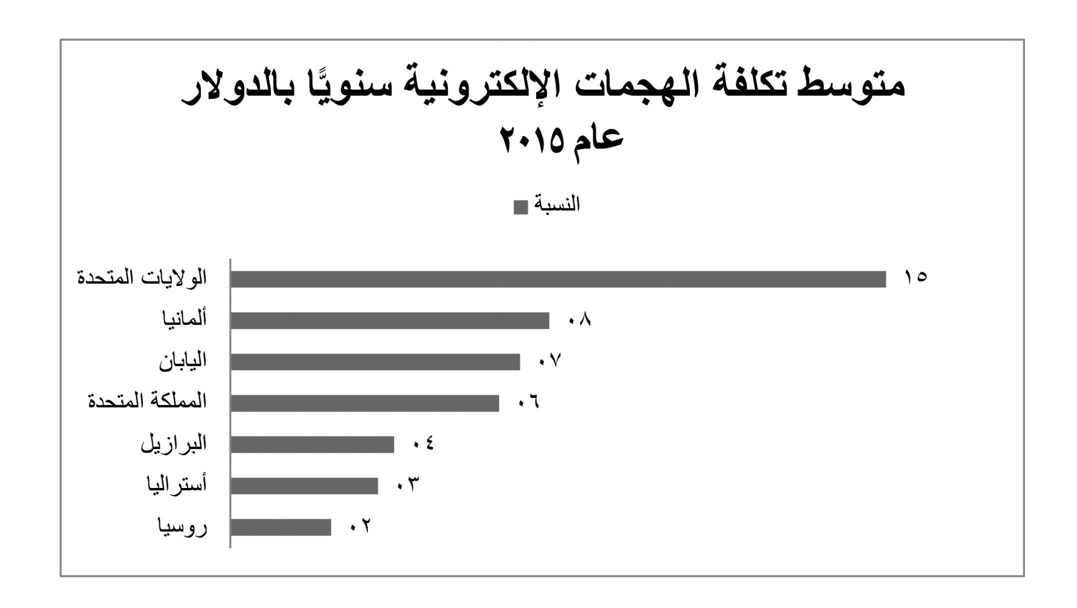
يلعب التسليح أهمية استراتيجية في توازن القوى وبسط النفوذ وتمكين الدول من ممارسة العديد من الأدوار والضغوط والتكتلات في ظل بيئة أمنية يمتلكها الشك وعدم اليقين ومصالح استراتيجية قابلة للتدمير في ثوانٍ معدودات، وهو ما يحمل خطورة عسكرة الفضاء الإلكتروني دون الأخذ بعين الاعتبار كونه يختلف عن ظروف التقدم في امتلاك الأسلحة النووية أو البيولوجية ودون الأخذ بالاعتبار حجم التدمير المنتظر وقوعه حال التعرض لهجوم إلكتروني، يمثل خطورة الإصابة الدولية من خطر استخدامها بالإضافة إلى تطويرها ونشرها والاستخدام السياسي للأسلحة الإلكترونية في الصراعات[٧٩].

إذا كان مجال الفيروس البيولوجي قد شهد سباقًا محمومًا في تطوير أسلحة بيولوجية، فإن الفيروس الإلكتروني قد أوجد كذلك تنافسًا بين العديد من الدول في الاستحواذ عليه وتطويره في إطار أسلحة الفضاء الإلكتروني والتي تحدد مصير أي معركة[٨٠]. وتبنت العديد من الدول استراتيجية حرب المعلومات باعتبارها حربًا للمستقبل، والتي يتم خوضها بهدف التشتيت وإثارة الاضطرابات في عملية صناعة القرارات عبر الدخول إلى أنظمة الطرف الآخر، استخدام ونقل معلوماته بعد الأهمية المتزايدة للفضاء الإلكتروني. وترى الدول الكبرى أن من يحدد مصير المعركة ليس من يملك القوة، وإنما القادر على شلِّ القوة والتشويش على المعلومة.

(٧٩) Neil Robinson *et al., Stocktaking Study of Military Cyber Defense Capabilities in the European Union (milCyberCAP): Unclassified Summary.* RAND Research Report 286 (Santa Monica, CA: RAND, 2013): 7.

(٨٠) E. Nakashima, “U.S. Accelerating Cyberweapon Research”, *The Washington Post*, online e-article, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html.

وتم استخدام الهجمات الإلكترونية في الصراع بين روسيا وإستونيا عام ٢٠٠٧، وفي الحرب الجورجية الروسية عام ٢٠٠٨، وفي الهجمات الإلكترونية على إيران من قبل إسرائيل والولايات المتحدة باستخدام فيروس ستاكس نت ضد المنشآت النووية الإيرانية، وقد كشف إدوارد سنودن عن قيام الولايات المتحدة بشن ٢٣١ هجومًا إلكترونيًا ضد روسيا وإيران والصين[٨١]. ودفع عجز حلف الناتو في مواجهة الهجمات الإلكترونية على إستونيا عام ٢٠٠٧ وجورجيا عام ٢٠٠٨ إلى تكوين مركز للدفاع الإلكتروني مقره تالين عاصمة إستونيا، وعمل على تطوير المفهوم الاستراتيجي للحلف بحيث أصبح الفضاء الإلكتروني منطقة لعمليات الحلف، وأن عليه أن يطور قدراته الدفاعية الإلكترونية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات إلكترونية، وأنه وفقًا لذلك فإن أي هجوم يتم على أوروبا أو أمريكا الشمالية يعتبر هجومًا ضد الجميع.



(٨١) "Latest Snowden leak: US mounted 231 Cyber-Attacks against Russia, Iran, and China", *The Voice of Russia: International* (31 Aug 2012), online e-article, http://sputniknews.com/voiceofrussia/news/2013_08_31/Latest-Snowden-leak-US-mounted-231-cyber-attacks-against-Russia-Iran-and-China-0260/.

وقام عدد من الدول بتشكيل وحدات للحرب الإلكترونية ضمن قواتها المسلحة، وقامت الولايات المتحدة بتشكيل قيادة عسكرية للفضاء الإلكتروني، وأصبحت تتجه بعض الدول إلى تخصيص ميزانيات للدفاع والأمن الإلكتروني.

واتجهت الدول لتعزيز دفاعاتها ضد خطر التعرض للهجمات الإلكترونية، ولكن الاتجاه الأكثر خطورة هو التحول من اتخاذ إجراءات وقائية ذات طابع دفاعي إلى الاتجاه إلى تبني سياسات هجومية.

وتبقى المشكلة في أنه عند دخول العالم سباق التسلح الإلكتروني A Cyber Arms Race يكون لدينا مشكلة في تحديد ماهية تلك الأسلحة التي يمتلكها الآخرون، ومن ثم لا يصبح لدى المجتمع الدولي قدرة سريعة على التدخل لاحتواء التقدم في مجال تلك الأسلحة، ولا يوجد مجال لتفعيل التفتيش كآلية مراقبة مثل حالة الأسلحة النووية.

وتشمل عملية بناء القدرات العسكرية في مجال الأسلحة الإلكتروني، السعي إلى امتلاك التكنولوجيا وأنظمة الحماية وتطوير قدرات هجومية، تعمل على تحقيق التفوق التقنيّ، والهدف الثاني، تطوير القدرات الهجومية إما عبر بناء القدرات الذاتية أو بالاستعانة بالأفراد والشركات المتخصصة وتطوير القدرة على اختبار مدى الجاهزية لمواجهة الهجمات الإلكترونية، والثالث، العمل على توفير الميزانيات المخصصة لتطوير القدرات الهجومية والدفاعية وبخاصة مع قلة تكلفتها مقارنة بحجم ما ينفق على الجيوش التقليدية.

وعلى الرغم من سرية النشاط المتعلق بالقدرات الإلكترونية فإن التوقعات تشير إلى أن هناك ما لا يقل عن ١٢٠ دولة تقوم بتطوير طرق للتجسس واستخدام الإنترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر الخاصة بالخدمات الحكومية. ومن أهم الدول التي تمتلك قدرات هجوم إلكترونية الولايات المتحدة والصين وروسيا وإسرائيل وفرنسا وبريطانيا والهند وألمانيا[٨٢].

---

(٨٢) Misha Glenny, "The Cyber Arms Race Is On, as Nations Large and Small Mobilize to Protect Themselves and Their Enemies If Provoked", *Pittsburgh Post-Gazette*, http://www.post-gazette.com/pg/11296/1183849-109-0.stm#ixzz1oMTYghXF.



واتهمت الولايات المتحدة مرارًا الصين باختراق شبكاتها الإلكترونية، واعتبرتها وروسيا خطرًا إلكترونيًا على أمنها[٨٣]، وتتهم الصين باختراق وكالة الفضاء الأمريكية NASA واختراق نظم المعلومات لأقمارها الصناعية في الفضاء الخارجي. وهو ما تنفيه الصين وتوجه نفس الاتهام مع إيران وروسيا للولايات المتحدة، وتعد كل من السويد وفنلندا وإسرائيل من أفضل الدول التي لديها جاهزية لمواجهة الهجمات الإلكترونية مقارنة بالولايات المتحدة وألمانيا وبريطانيا[٨٤].

وتجري الولايات المتحدة سنويًّا محاكاة التعرض لحرب إلكترونية فيما يطلق عليها بعاصفة الحواسب Cyberstorm وخصصت ٥٠٠ مليون دولار في ميزانية عام ٢٠١٢ لمواجهة التهديدات الإلكترونية، وعملت على تطوير أسلحة وأدوات للحرب الإلكترونية تشمل فيروسات قادرة على تخريب شبكات العدو الحساسة، وذلك لتحسين درجات الاستعداد لحرب الكمبيوتر[٨٥].

وأعلنت الولايات المتحدة عن جهود تصنيع لأسلحة إلكترونية هجومية لمواجهة احتمال تعرضها لهجوم، وعملت على زيادة مخصصات تمويل الأبحاث الإلكترونية من ١٢٠ مليون دولار إلى ٢٠٨ ملايين دولار عام ٢٠١٢، وتبلغ تكلفة الهجمات الإلكترونية ١١ بليون دولار و٩ ملايين مواطن تم اختراق خصوصياتهم وتكلفت الجريمة الإلكترونية ٣,٨ بليون دولار. وأعلنت روسيا عزمها على تطوير السلاح الجوّي والفضائي ردًّا على الدرع الصاروخية وخصصت ٥٩٠ مليار يورو لإعادة التسليح خلال العقد المقبل والعمل على استعادة موقع الزعامة في التكنولوجيّات العسكرية[٨٦]. وقامت إيران بتأسيس مقر الدفاع الإلكتروني في أكتوبر ٢٠١١، وأصبحت من ضمن الدول التي تملك منظومة دفاعية كاملة

---

(٨٣) Dan Raywood, “US Says China and Russia are Cyber Threats”, *CRN News*, http://www.crn.com.au/News/279216,us-says-china-and-russia-are-cyber-threats.aspx.

(٨٤) Brigid Grauman, “Cyber-Security: The Vexed Question of Global Rules”, *Friends of Europe*, http://www.friendsofeurope.org/security-europe/3110/.

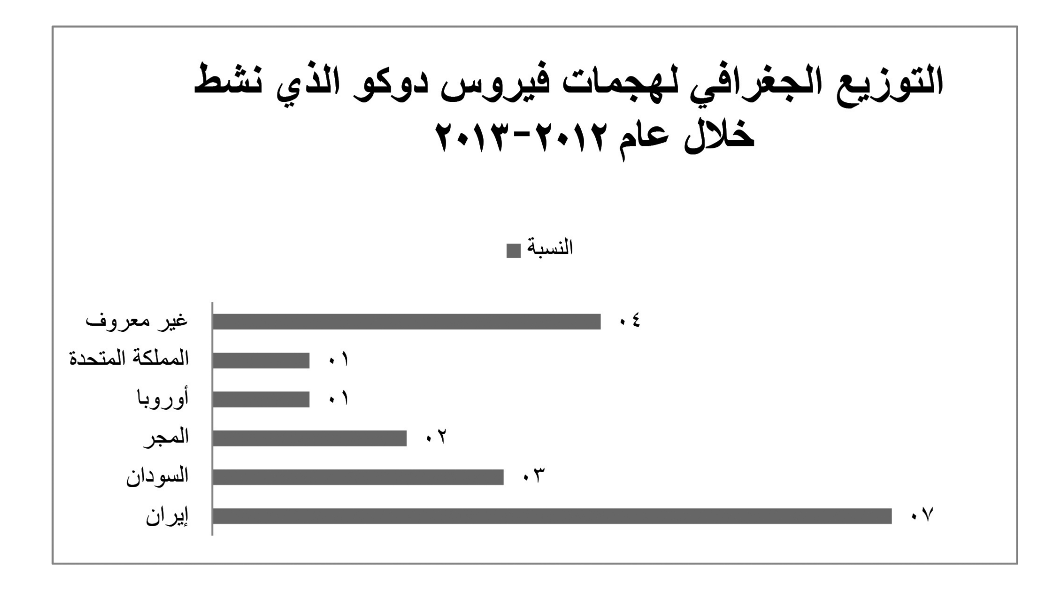
(٨٥) Ellen Nakashima, “List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare”, *The Washington Post* (1 June 2011), online e-article, https://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_print.html.

(٨٦) «بوتين يُطلق سباق التسلّح مع الغرب»، **الجزائر نيوز** (٢٠ فبراير ٢٠١٢)، مقالة إلكترونية متاحة عبر الإنترنت، http://www.djazairess.com/djazairnews/35239.



في مواجهة تهديدات الحرب الإلكترونية، وظهر في نجاح إيران في احتواء فيروس دوكو في بداية عام ٢٠١٢ بعد ساعة من إطلاقه.

وأنشأت إسرائيل وحدة خاصة تدعى «رام» لمواجهة حملات الغزو الإلكتروني والدفاع عن المواقع الاستراتيجية، وأنشأت وحدات متخصصة في تكنولوجيا المعلومات والشبكات الاجتماعية كموقع فيس بوك على الإنترنت كسلاح استراتيجي في الجيش. إلى جانب وحدة تسمى «٨٢٠٠» التابعة لوزارة الدفاع الإسرائيلي في حرب الإنترنت. وقامت الحكومة البريطانية بتطوير برامج أسلحة إلكترونية، من شأنها أن تعزز الخيارات الهجومية، إلى السياسات الدفاعية، وأقرت بأنها جزء لا يتجزأ من ترسانة الأسلحة البريطانية، وهو ما يمثل أول اعتراف رسمي بوجود مثل هذه البرامج الإلكترونية[٨٧].



المصدر : تقرير شركة كاسبرسكي ٢٠١٤

---

(٨٧) ريم عبد الحميد، «الجارديان: الحكومة البريطانية تطور أسلحة هجوم إلكتروني»، **اليوم السابع: صحف عربية وعالمية** (٣١ مايو ٢٠١١)، مقالة الكترونية متاحة عبر الانترنت، http://www.youm7.com/story/2011/5/31/424640/الجارديان--الحكومة-البريطانية-تطور-أسلحة-هجوم-إلكتروني.

وأعلنت روسيا اعتزامها إنشاء وحدات دفاع «سيبراني–إلكتروني» لحمايتها من الحرب على الإنترنت خلال السنوات القادمة، وذلك على مراحل حتى حلول عام ٢٠١٧. وللدفاع عن البنية التحتية للقوات المسلحة الروسية، وقام الجيش بتجنيد عدد كبير من المبرمجين الجدد لدعم البرامج العسكرية، بالإضافة إلى إمكانية التعاون مع جماعات القراصنة.

وبلغ الإنفاق العسكري الروسي على حرب الفضاء الإلكتروني ١٢٧ مليون دولار من إجمالي إنفاق عسكري بلغ ٤٠ بليون دولار في روسيا، التي تحتل المركز الرابع عالميًّا في مجال تطوير قدرات الأسلحة الإلكترونية. في حين تأتي الصين في المركز الثاني عالميًّا في مجال تطوير قدرات حرب الفضاء الإلكتروني، وتبلغ ميزانية الإنفاق عليها ٥٥ مليون دولار من جملة إنفاقها العسكري البالغ ٦٢ بليون دولار. وهناك العديد من الدول التي تعكف على تطوير ترسانة الأسلحة الإلكترونية(٨٨).

ومن ناحية أخرى تتهم اليابان كلاً من روسيا والصين وكوريا الشمالية باستهدافها بالهجمات الإلكترونية، وهو ما دفع اليابان إلى تطوير قدراتها الإلكترونية بتطوير فيروسات لملاحقة وتعطيل مصادر الهجمات الإلكترونية التي تشن ضدها وحصل العملاق Fujitsu على حقوق هذا المشروع بتكلفة ٢,٣ مليون دولار في خطة عمل ٣ سنوات. وهو ما يدفع لإجراء تعديلات دستورية وقانونية تصرح باستخدام أسلحة إلكترونية ويمنع القانون الحالي تبني سياسات هجومية(٨٩).

وقامت الصين التي تعد أول دولة في العالم تنشئ وحدة خاصة بالحرب الإلكترونية بتطوير أسلحة نبض كهرومغناطيسية؛ لاستخدامها ضدَّ حاملات الطائرات الأمريكية في أي صراع مستقبلي حول تايوان. وهي تشبه نبض أشعة جاما، الناجمة عن تفجير نووي بما يتسبَّب في تعطيل كلِّ الأجهزة الإلكترونية، بما في ذلك أجهزة الحاسب الآلي وغيرها على مساحات واسعة. إن الأسلحة الإلكترونية الصينية تعد جزءًا مما يعرف بمشروع أسلحة «الورقة الرابحة» لدى الصين، والتي تعتمد على التكنولوجيا الحديثة التي يجري تطويرها في

---

(٨٨) Kevin G. Coleman, *"The Cyber Arms Race Has Begun"*, CSO: Opinion. http://www.csoonline.com/article/2122353/critical-infrastructure/coleman--the-cyber-arms-race-has-begun.html.

(٨٩) "Japan Developing Cyber Weapon: Report", *The Australian Business Review* (2 Jan 2012), online e-article.

مستوى عالٍ من السرية[٩٠]. وعلى الرغم من إعلان الصين أنها لن تدخل في سباق تسلح مع أي دولة، فإنها رفعت الإنفاق العسكري من ١١٩,٨ مليار دولار في ٢٠١١ وبزيادة قدرها ١١,٢٪ عام ٢٠١٢ ومتوقع أن تصل إلى ٢٣٨,٢ مليار دولار في ٢٠١٥.

وتواجه الولايات المتحدة تحديًا في قيادة الدول الأخرى فيما يتعلق بالقدرات السيبرانية، ومن ضمنها المتنافسون في آسيا والمحيط الهادي، وهو ما يضع ضغطًا كبيرًا على الولايات المتحدة وصانعي القرار بها للتعامل مع عملية انتشار القدرات السيبرانية الهجومية سواء من جانب الدول أو من غير الدول، وهو ما يختلف عن عملية التطور في الصواريخ الباليستية وتعتمد الأسلحة الإلكترونية على المعرفة والشفرات[٩١].

وتمتلك الصين وإيران وكوريا الشمالية وروسيا قدرات إلكترونية هجومية، والتي يمكنها أن تشكل خطرًا على الولايات المتحدة وحلفائها، حيث عبرت عملية السباق الإلكتروني في مجال التسلح عن خريطة الصراع والتنافس ما بين القوى الكبرى، كما يتم بين باكستان والهند وما بين الصين واليابان وما بين إسرائيل والعالم العربي، ويزداد الأمر خطورة إذا ما تم نشر تلك القدرات في السوق السوداء، والتي يمكن أن تقع في أيدي الجماعات الإجرامية التي تهدف إلى الحصول على المال، أو الإرهابية التي تسعى إلى الاستخدام السياسي لها أو رغبة دول أخرى في امتلاكها ولا تستطيع أن تنتجها مثل تلك القدرات السيبرانية، وهو ما يوفر بيئة مثالية لعلاقة البائع والمشتري في السوق السوداء، وهو ما يحمل خطورة وتأثير على القدرات الأمريكية في مجال الأسلحة الإلكترونية من خلال العمل على تضييق الفجوة بينها وبين غيرها من الدول الأخرى، وهو ما يهدد القدرات السيبرانية للولايات المتحدة، ويضع مفهوم الهيمنة في حالة مراجعة إذا ما تم تطبيقه في المجال الإلكتروني عندما يتمكن مراهق يبلغ ١٦ عامًا من شن هجمات إلكترونية مؤثرة.

---

(٩٠) «الصين تطور أسلحة جديدة قادرة على شل حركة حاملات الطائرات الأمريكية»، **الصين بعيون عربية**، http://www.chinainarabic.org/?p=3039.

(٩١) Eddie Walsh, “The Cyber Proliferation Threat”, *The Diplomat,* http://thediplomat.com/2011/10/the-cyber-proliferation-threat.

وتتفوق الولايات المتحدة في أولويات الاستثمار في تطبيقات الأمن الإلكتروني الدفاعية عن بقية دول العالم، ولكنها تواجه صعوبة في وضع إطار للحماية لكل هدف محتمل للهجوم بخلاف الفضاء، فإن عدد الأهداف المحتملة غير محددة وغير مقيدة بالجغرافيا، وتركز الولايات المتحدة من ناحية أخرى على الاستثمار في نشر القدرات الهجومية على اعتبار أن الهجوم هو أفضل وسيلة للدفاع، وهو ما يحاط بقدر كبير من السرية، وهو ما يضع صعوبة في معرفة حقيقة تلك القدرات وقوتها وحجمها، وتهدف القدرات الهجومية تحقيق نوع جديد من الردع في المجال الإلكتروني، والتي تقود عملية الاستثمار في هذا الفضاء، وتضع الولايات المتحدة أهمية قصوى في حماية شبكاتها.

وتمثل عملية نمو القدرات السيبرانية الهجومية للدول الخارجية خطرًا على أمن الولايات المتحدة إلى جانب انتشار الأسلحة النووية، وأنه في حال امتلاك أعداء الولايات المتحدة لمثل تلك القدرات يمكنها أن تشكل خطرًا محدقًا بأمنها، وتهتم الولايات المتحدة ليس فقط بعمليات الدفاع والهجوم في المجال الإلكتروني بل باستخدام الفضاء الإلكتروني في شن دبلوماسية فاعلة لتحقيق أهدافها الخارجية[٩٢].

وتوجه الولايات المتحدة اتهامًا للصين بشنِّ هجمات الفضاء الإلكتروني في إطار جزء من خطط بكين لفرض «هيمنة إلكترونية» على خصومها العالميين بحلول عام ٢٠٥٠ في مواجهة الولايات المتحدة وبريطانيا وروسيا وكوريا الجنوبية. وفيما يتعلق بحالة الإنفاق العسكري على الأسلحة الإلكترونية[٩٣] تشير إلى وجود خمس دول كبرى في مجال امتلاك القدرات الإلكترونية في مجال الفضاء الإلكتروني، وفي عام ٢٠١٢ بلغت ميزانية تطوير القدرات الإلكترونية الدفاعية لحلف الناتو ٥٨ مليون يورو، وفي الولايات المتحدة والتي وصلت ميزانية الدفاع الإلكترونية إلى ١,٥٤ بليون دولار في المدة من ٢٠١٣–٢٠١٧.

(٩٢) Zachary K. Goldman, "Washington›s Secret Weapon Against Chinese Hackers: Applying the Lessons of Counterterrorism and Counterproliferation in Cyberspace", *Foreign Affairs* (8 Apr 2013), online e-article, https://www.foreignaffairs.com/articles/united-states/2013-04-08/washingtons-secret-weapon-against-chinese-hackers.

(٩٣) Pierluigi Paganini, "The Rise of Cyber Weapons and Relative Impact on Cyberspace", *InfoSec Institute,* http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace.



وفي المملكة المتحدة بلغت ميزانية تطوير الفيروسات الدائية والمخترقين ٦٥٠ مليون جنيه إسترليني، وفي المركز الرابع أنفقت إسرائيل ١٣ مليون دولار في تطوير التكنولوجيا الجديدة في مجال الدفاع الإلكتروني، وفي الصين والتي تفرض غموضًا على نفقاتها التسليحية إلا أن بعض التقديرات تشير إلى إنفاقها في عام ٢٠١١ ما بين ١٢٠ مليون دولار إلى ١٨٠ مليون دولار، ومن المتوقع أن ترتفع من ميزانية ١,٨ بليون دولار في عام ٢٠١١ إلى ٥٠ بليون دولار عام ٢٠٢٠ وبزيادة سنوية تصل إلى ٤٤,٧٪، وأعلنت إيران عن طموحها في تحسين قدراتها في مجال الحرب الإلكترونية، وقامت بتأسيس فريق معني بذلك، ووصل حجم الإنفاق إلى بليون دولار عام ٢٠١٢.

ويلاحظ أن الصين والولايات المتحدة قد خصصتا استثمارات كبيرة لتطوير تقنيات الإنترنت الجديدة. وعلى الرغم من أن المبالغ المخصصة قد تبدو باهظة فإنها رخيصة مقارنة مع تكلفة سلاح تقليدي، وهو ما دفع كثيرًا من الدول إلى إنشاء وحدات للإنترنت مخصصة لتطوير تكنولوجيات الهجوم الإلكتروني.

وتعتمد تكلفة الأسلحة الإلكترونية على عوامل متعددة، وبخاصة البعد الاقتصادي الذي يتعلق بالقدرة على الحماية ومنع التجسس أو ترسيب الأسرار الصناعية إلى الخارج بما يكلف الدولة ملايين الدولارات، وهو ما يدفع إلى أهمية تبني استراتيجية إلكترونية سليمة، وبخاصة فيما يتعلق بالقدرة على تطوير ترسانة الأسلحة الإلكترونية. بالنظر إلى أن عملية تطوير الأسلحة الإلكتروني يكتنفها نوع من السرية والغموض كشأن نفقات التسليح والدفاع في دول العالم المختلفة، والتي يصعب معرفتها بدقة، والتي قد تقتصر فقط على صفقات السلاح المعلنة، ومن ثم فإن التسلح الإلكتروني باعتباره مجالاً جديدًا في أنظمة التسليح فإنه يحظى بقدر عالٍ من السرية والاهتمام في الاستثمار في تطويرها.

ومن ثم يصعب تحديد التكلفة بدقة لتطوير أسلحة إلكترونية لكونها تعتمد كذلك على عدد كبير من المتغيرات، ووضع تشارلي ميلر القرصان الشهير مخططًا لميزانية لإقامة جيش إلكتروني أمريكي، واقترح أن تبلغ مدة المشروع عامين يضم حوالي ٥٩٢ من المختصين في مختلف الأدوار المهمة من المحللين والمديرين والتقنيين، ويشير إلى أن تطوير السلاح

السيبراني يحتاج مهنيين ذوي المهارات العالية، وتبلغ التكلفة ما يزيد على ٤٥,٩ مليون دولار في الراتب السنوي، متوسط الراتب السنوي ٧٧٥٣٤ و٣ ملايين دولار...[٩٤].

وفي ٢٠١٤ قدمت هيئة الدفاع الوطني الأمريكية مشروع قانون للكونجرس لطلب الموافقة عليه، والذي يهدف إلى تنظيم انتشار الأسلحة الإلكترونية، وفي نفس الوقت توفير ميزانية ضخمة لتطوير تلك الأسلحة، ودعت مبادرة الأمن الإلكتروني لمواجهة التجارة الدولية في مجال الأسلحة الإلكترونية، والتي يمكن أن يتم استخدامها لمواجهة الجماعات الإرهابية والإجرامية والنشاطات العسكرية، ودعم حق الدول في استخدام تلك الأسلحة كأداة للدفاع الشرعي عن النفس[٩٥].

ودعا مشروع القانون الرئيس الأمريكي إلى العمل على إنشاء عملية مشتركة بين الوكالات المعنية، للعمل على توفير عملية وضع سياسة متكاملة، للسيطرة على انتشار الأسلحة الإلكترونية إما من خلال القيام بأنشطة من جانب واحد أو من خلال تعزيز التعاون لتنفيذه، والوسائل المالية، والعلاقات الدبلوماسية، وغيرها من الوسائل الأخرى، التي يمكن أن يراها الرئيس مناسبة، وقد تمت المطالبة بتخصيص ٦٨مليون دولار للقيادة العسكرية للفضاء الإلكتروني، و١٤ مليون دولار لدعم برنامج الهجوم في عمليات القوات الجوية، و٥,٨ مليون دولار للدفاع الإلكتروني، و١٩ مليونًا لأبحاث الأمن الإلكتروني، و٢٠ مليون دولار لدعم الأبحاث المتقدمة في الأمن الإلكتروني، و١٦٩ مليون دولار لاستكمال إنشاء مبنى مركز العمليات في الفضاء الإلكتروني[٩٦]، وقد ترددت كلمة «السيبر» اثنتي عشرة مرة في مشروع مخصصات الدفاع عام ٢٠١٢، وواحدًا وستين مرة في وثائق الميزانية لعام ٢٠١٣، و١٢٧ مرة في مسودة قانون الميزانية لعام ٢٠١٤.

(٩٤) Stefano Mele, *Cyber Weapon: Legal and Strategic Aspects (Version 2.0)* (Rome: Italian Institute of Strategic Studies “Niccolò Machiavelli”, 2013), online e-book, http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf.

(٩٥) USA, Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (USA: Office of the Secretary of Defense, 2013), online e-book, http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf.

(٩٦) Anthony M Freed, “US Defense Budget to Both Regulate and Proliferate Cyber Weapons”, *Tripwire: The State of Security,* http://www.tripwire.com/state-of-security/top-security-stories/us-defense-budget-regulate-proliferate-cyber-weapons.



مع زيادة الاهتمام الأمني بالبنية التحتية الحيوية مثل أنظمة الدفاع القومية وصناعات أنظمة التحكم وشبكات الاتصالات، ساعد ذلك في نمو سوق الأسلحة الإلكترونية وبذلك ظهر الفضاء الإلكتروني كمجال جديد للحرب مثل البر والبحر والجو، ودفع ذلك العديد من الفاعلين من الدول إلى تبني تطوير تلك الأسلحة بجهودها الذاتية أو عبر الاستعانة بشركات تكنولوجية متقدمة، أو عبر استعانة بالقراصنة وبالسوق السوداء لتجارة تلك الأسلحة غير الخاضعة للرقابة، وأشار تقرير لمركز شفافية السوق[٩٧] إلى تصاعد الاهتمام العالمي بالأسلحة الإلكترونية – السيبرانية، وتوقع التقرير أن يتسع السوق العالمي لتجارة الأسلحة الإلكترونية بنسبة ٤,٤٪ من عام ٢٠١٥ إلى عام ٢٠٢١.

وفي معدل النمو ذلك من المتوقع أن يصل تقييم حجم السوق من ٥٢١،٨٧ بليون دولار أمريكي بحلول عام ٢٠٢١، وبزيادة عن عام ٢٠١٤ والتي وصل فيها إلى ٣٩٠ بليون دولار. وهذه القيمة مرشحة للزيادة مع تصاعد أخطار الهجمات الإلكترونية، والتي فرضت ضرورة تطوير الأسلحة الإلكترونية للدفاع، إلى جانب اهتمام الحكومات وأجهزة الاستخبارات بالتطوير في مجال الحرب السيبرانية الهجومية والقدرة على امتلاك قدرات احتواء الهجمات الإلكترونية. وهو ما من شأنه أن يعمل كذلك على نمو الطلب في سوق الأسلحة السيبرانية الهجومية، وإلى جانب الدول الكبرى التي تعمل على نمو قدراتها هناك عدد من الشركات التقنية التي تعمل على تطوير الصناعة العالمية للأسلحة السيبرانية، ومن تلك الشركات شركة لوكهيد مارتين وشركة بوينج وايرباص وشركة BAE وشركة ريثون وشركة نورث روب جرومان[٩٨].

وفيما يتعلق بالسوق العالمي للأسلحة السيبرانية جغرافيًا ففي أمريكا الشمالية توجد الولايات المتحدة وكندا والمكسيك، وفي أوروبا توجد المملكة المتحدة وألمانيا وفرنسا وباقي أوروبا، وفي منطقة آسيا المحيط الهادي توجد الهند والصين واليابان وباقي دول المنطقة، وباقي العالم مثل أمريكا اللاتينية والشرق الأوسط وإفريقيا.

(٩٧) "Cyber Weapon Market – Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2015 – 2021", *Transparency Market Research*, http://www.transparencymarketresearch.com/cyber-weapon-market.html.

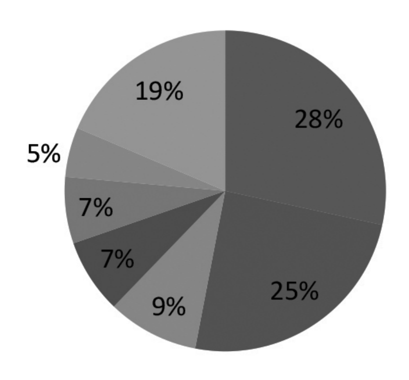
(٩٨) Lockheed Martin Corporation, BAE Systems plc, General Dynamics Corporation, Airbus Group SE, The Boeing Company, Raytheon Company, and Northrop Grumman Corporation.

ويشمل سوق الأسلحة السيبرانية نمطين أساسين؛ الأول يتعلق بالأسلحة الدفاعية، والأخرى تتعلق بالأسلحة الهجومية، وفيما يتعلق بحجم السوق وفقًا إلى التطبيقات توجد أنظمة الدفاع القومي وشبكات اتصالات ونظم التحكم الصناعي والخدمات المالية والبنكية، وأجهزة التحكم في المجال الجوي، ونظم المواصلات الذاتية، والمستشفيات.

كبرى الشركات العاملة في مجال الأسلحة الإلكترونية ونصيبها من السوق العالمي

Market Share Range (2011)

- European Aeronautic Defence and Space Company EADS N.V
- The Boeing Company
- United Technologies Corporation
- General Electric Company
- Bombardier INC
- Rolls-Royce PLC
- Other



المصدر: تقرير لشركة بوينج لعام ٢٠١١

المبحث الثالث

أثر الفضاء الإلكتروني في القانون الدولي العام وقانون الحرب

أولاً: أثر العلم والتكنولوجيا في علم القانون الدولي

ترتبط العولمة بما هو دولي أو عالمي، وتشير إلى تحول العالم لقرية كونية أو عالمية Global Village ويدور مفهوم «العولمة» حول الوجود العالمي أو الانتشار الكوني، حيث تترك تجلّياتها تأثيرًا عميقًا على التفاعل الإنساني على الأصعدة السياسية والاقتصادية والاجتماعية والثقافية، وفي إطارها النظري تعدو لتزايد التبادل والاعتماد المتبادل بين الدول، وإدارة المصالح المشتركة للبشرية ولصالح البشرية، وتبدو وكأنّها أصبحت ضرورة لا غنى عنها للتعامل مع كثير من القضايا البشرية، خصوصًا بعد أن اتسعت دائرة الاهتمام بحقوق الإنسان وتشابكت على المستوى الكوني، وأصبحت جزءًا من القانون الدولي[٩٩].

وحققت العولمة، اتجاهًا متعاظمًا نحو تخطي الحدود الجغرافية وتجاوز القيود السياسية، والقدرة الممكنة على التقاط الثقافات وتبادل التجربة الإنسانية في المجتمعات المختلفة، وعدم الأخذ بعين الاعتبار الانتماء إلى وطن محدد أو دولة معينة، وكل ذلك بفعل التطور التكنولوجي والإعلامي والمعرفي عمومًا، وما رافقه من اختصار لعوامل المسافة والزمن، وهو ما ينفي الحاجة إلى التقيد بالإجراءات الحكومية الرسمية، وهو ما يقود طبيعيًّا إلى إسقاط القوانين بكل ما تعنيه هذه القوانين من ضبط للأداء الإنساني في أبعاده وأنماطه الاجتماعية العامة، والتي تعطي للثقافة هويتها الخاصة، وللهوية ثقافتها الخاصة.

وللعولمة شقان: أولهما: شق مادي ملموس نشأ نتيجة التطور العلمي والتكنولوجي، وثورة المعلومات من خلال وسائل الاتصال والإعلام، وانتشار المحطات الفضائية التي تعم برامجها كل أرجاء الكرة الأرضية، وتصل نسبيًّا إلى غالبية البشر، وثانيهما: شق قيمي نشأ نتيجة التوسع التنافسي للإنتاج الرأسمالي الذي فرض اقتصاد السوق على العالم، وساعد

---

(٩٩) سعيد حسين محمود حسن غلاب، **التطورات الراهنة في النظام الدولي وأثرها على مبدأ حظر استخدام القوة في العلاقات الدولية** (رسالة دكتوراه، جامعة القاهرة. كلية الاقتصاد والعلوم السياسية، ٢٠٠٥): ٣٠٠–٣٢٧.



الانتشار السريع لتكنولوجيا الاتصال والمعلومات من حركة الاعتماد المتبادل بين دول العالم على المستوى الاقتصادي، وأهمية دورها في النمو الاقتصادي العالمي المتمثل في الاقتصاد الرقمي على حساب القطاعات الأخرى التقليدية في الاقتصاد، وكان لذلك تأثير على دور الدول وتأثيرها في العلاقات الدولية؛ حيث جاءت التغيرات في البيئة الدولية من جراء اعتماد الاقتصاد على المعرفة وتدفق المعلومات بدلاً من الاعتماد على المواد الخام أو الموارد الطبيعية أو التجارة.

وأصبح لتكنولوجيا الاتصال والمعلومات دور في دعم التجارة الإلكترونية، وتقديم الخدمات الحكومية، وعمل المؤسسات المالية، وتقديم الخدمات الحكومية، إلى أن أصبحت بمثابة عصب التقدم والحياة المعاصرة، وكان لذلك تأثيرات على سيادة الدول بعد أن اجتازت الشبكات الحدود التقليدية للدول وعملت على الانتقال الحر والسريع للمعلومات من الدول وإلى الخارج والعكس بدون عوائق جمركية أو سيادية، وحدث تراكم جديد للثروة وإعادة توزيع للقوة بين دول العالم، وأصبحت المعرفة والمعلومات هي مصدر الثروة مع قلة الاعتماد على القوة العسكرية والموارد الطبيعية كمصادر للقوة.

وأحدثت الثورة التكنولوجية تغييرات في الشئون العسكرية؛ حيث أثرت على المعرفة الكاملة بالذات والخصم بما يظهر في الوعي الكامل بميدان المعركة، وعملت على تعقد الجهود لمسألة التفريق ما بين الأهداف العسكرية والأخرى المدنية، وهذا بالإضافة للمساعدة على إمكانية إحداث الضرر البالغ بالمدنيين والمنشآت، وبما مثل خطرًا على الالتزام بقانون النزاعات المسلحة(١٠٠). أما على صعيد القانون الدولي ذاته فلم يعد قانون دول بل قانون علاقات دولية، وأصبح هناك فواعل لم ترقَ بعد إلى مرتبة الشخص القانوني الدولي إلا أنها أكبر مؤثر في صنع القاعدة القانونية بطريقة ما؛ فالقانون أصبح يحكم مجمل علاقات الدول ووحداتها، وحدث للمصادر الشكلية للقانون الدولي تطور من جراء ثورة

(١٠٠) Bryan W. Ellis, *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?* (Pennsylvania: U.S. Army War College. Carlisle Barracks, 2001).



تكنولوجيا الاتصال والمعلومات، وهناك فجوة واضحة بين القواعد المنظمة للعلاقات الدولية والممارسة الفعلية لأعضاء النظام الدولي(١٠١).

وجاء ذلك ضمن التحديات السياسية والاقتصادية والأمنية والقانونية التي فرضتها التغييرات التكنولوجية والاتصالية أمام القانون الدولي، الذي تعامل أساسًا مع مفاهيم القوة الصلبة واستخداماتها، واتسم بالجمود والمحافظة – منذ اتفاقية ويستفاليا ١٦٤٨ – وتراجع في حيثياته وأطره القانونية أمام تصاعد القوة اللينة، والتي أفضت إلى أنشطة جديدة لم تتوافق مع تلك الأطر، أو أنها كشفت عن تناقضها مع تلك المبادئ القانونية الموجودة، أو أنها كشفت أن هناك بعض القواعد القانونية التي يمكن تطبيقها في مبادئها العامة، كما في اتفاقيات جينيف لعام ١٩٤٩ والبروتوكولات المكملة لها في عام ١٩٧٧ والقانون الدولي العرفي، وحتى إن اتفاقية جينيف ركزت على حماية الأشخاص وقت الحرب دون الإشارة إلى أسلحة محددة، ولم يقدم البروتوكولان الإضافيان إشارة إلى طرق وأنواع الحرب المختلفة إلا في خصائصها العامة.

وكانت الاتفاقيات الأصلية التي وقعت عام ١٨٦٤ ثم طورت عام ١٩٤٩تعاملت مع مفهوم واحد للحرب، وهي الحرب التي تخوضها الجيوش النظامية بين الدول القائمة، عاكسة بذلك طبيعة الصراع الذي ظهر في أوروبا ابتداءً من الحرب النابليونية إلى الحرب العالمية الثانية، غير أن هذه الحروب أصبحت هي الاستثناء، كما أن طبيعة التهديدات الإرهابية قد أوجدت نوعًا جديدًا من الحروب لا تنطبق عليه اتفاقيات جنيف، بل تجعل تلك الاتفاقيات على نحو ما، وكأن الزمن قد تجاوزها، ومثل هذه المجادلات تشير إلى قدر أوسع من الشك في مدى استخدام اتفاقيات جنيف وآخذًا في الاعتبار تغيير طبيعة الحروب والمشاركين في هذه الحروب.

وأظهرت الثورة التكنولوجية الفجوة بين القواعد القانونية التقليدية وما بين التطور في النظام الدولي، ومع التنامي المستمر في ظاهرة الاعتماد الدولي في بعده الاقتصادي والأمني

---

(١٠١) أحمد عبد الونيس، **العولمة والقانون الدولي**، تحرير حسن نافعة، وسيف الدين عبد الفتاح، سلسلة محاضرات الموسم الثقافي الأول، (القاهرة: جامعة القاهرة. قسم العلوم السياسية، ٢٠٠٠).

والسياسي، وانتقل القانون الدولي من قانون تشكل نواته الدولة إلى مرحلة جديدة بني فيها على فكرة الصالح المشترك للجماعة الدولية ككل، ولينتقل من التعبير عن مصالح جماعة دولية محدودة.

وظهرت تحديات غير تقليدية للمجتمع الدولي، ولتتسع لتشمل الأمن الإنساني بمفهومه الشامل كحماية حقوق الإنسان ومكافحة التلوث والإرهاب الدولي وقضايا الاحتباس الحراري وغيرها، وتميزت تلك القضايا ببعدها الدولي وتعديها للحدود الوطنية، وطرأ تغير على مفهوم سيادة الدول وعدم التدخل في شئونها الداخلية والحق المشروع في استخدام القوة، وكانت تلك المبادئ تمثل روح القانون الدولي التقليدي ومحور قواعده الدولية.

كما تغيرت طبيعة الحرب والعدوان والإرهاب، ولم يقتصر التطور الذي شهده القانون الدولي في قواعده وأشخاصه بل ظهر أيضًا في مجاله[١٠٢]. وأصبحت الحروب تتراوح بشدة بين صراعات غير متوازنة تضع جيوشًا مدربة تدريبًا راقيًا ومجهزة بأحدث الوسائل التكنولوجية، أمام مقاتلين غير نظاميين يركبون الخيول وبين صراعات يتداخل فيها أشباه العسكريين والمجرمين، والطابع المدني بالعسكري. وظهرت الحروب الحديثة والمقاتلون الجدد، والاستخدام العسكري للأهداف المدنية، وجاءت اتفاقيات جنيف لتتعامل مع الجيوش التقليدية، بينما تفرض الحروب الحديثة تحديات عدم وجود خطوط قانونية واضحة تحمي هؤلاء الذين يتم القبض عليهم في الصراعات، كما أن هذه الخطوط العريضة لا تحترم من قبل المشاركين في وضعها سواء من الدول أو من غير الدول ومن ضمنهم المحاربين في حرب العصابات والجماعات التي تستغل الأطفال في الحروب[١٠٣].

ودفعت تلك التغييرات لإعادة النظر في اتفاقيات جنيف بشأن الأسرى؛ لأنها غير قادرة على التعامل مع تلك التطورات، وأصبح العالم وفقًا لوجهة النظر الحربية لم يعد فيه بالضرورة تحارب الدول بعضها البعض، بل أصبح هناك محاربون غير شرعيين دون الدولة، ومن ثم لا ينطبق عليهم اتفاقيات جنيف بشأن الأسرى، فالإرهابيون يعاملون كأسرى حرب، ومن ثم

(١٠٢) إسماعيل صبري مقلد، **نظريات السياسة الدولية: دراسة تحليلية مقارنة**، ط. ٢ (الكويت: ذات السلاسل، ١٩٨٧): ١١–٦٤.

(١٠٣) Renee de Nevers, "Modernizing the Geneva Conventions", *The Washington Quarterly 29*, no. 2 (2006).

فلهم حقوق الأسرى وفق اتفاقيات جينيف على الرغم من أنهم محاربون غير شرعيين؛ لأنهم ليسوا بأعضاء في جيش نظامي ولا يرتدون زيًّا عسكريًّا.

وظهرت إشكاليات تتعلق بمسألة تحديد الأهداف المدنية والأهداف العسكرية وتعريف العدوان وتعريف الحرب وحماية المدنيين والأماكن التي تستحق الحماية، وتحديد ضرب الأهداف المشروعة والتمييز بين الأهداف العسكرية والمدنية، ومدى القدرة على تقليل حجم الأضرار وقت الحرب أو التهديد بشأن استخدامها، وجاءت التغيرات التكنولوجية بأنشطة جديدة لا يوجد تكييف قانوني واضح يلائمها في الأطر القانونية الحالية أو أنها كشفت عن التعارض ما بين القوانين الدولية القائمة، بالإضافة إلى بروز مشكلات تتعلق بوضعها القانوني(١٠٤).

وأصبحت الحرب في العصر الحديث لا تشبه إلا في أقل القليل المعارك التي كانت تدور بين جيوش متكافئة بقدر أو بآخر، ويتقابل فيها جنود يرتدون الزى العسكري، وينتمون إلى دول بينها عداء، وقد وضعت اتفاقيات جينيف خصيصًا لها، ومسألة تحديد الأهداف المدنية والعسكرية وتعريف العدوان والحرب وحماية المدنيين والمنشآت التي تستحق الحماية، ومدى القدرة على تقليل حجم الأضرار وقت الحرب، ومثل ذلك خطرًا على الالتزام بقانون النزاعات المسلحة، وفرض تغييرات في الإطار القانوني والمبادئ التي يقوم عليها ونطاقه ووسائل تطبيقه والأشخاص المحميون والقواعد الأساسية للنزاعات المسلحة والمسئولية المترتبة على خرق القانون وطبيعة الانتهاكات والجزاء والعقاب(١٠٥).

وفرض الاستخدام السلبي للتقدم التكنولوجي تحديات في سبيل معالجة القانون الدولي، وأصبح هناك تأثير متبادل بين التقدم التكنولوجي وما يفرزه من تحديات وقدرة القانون الدولي على التكيف معها(١٠٦).

---

(١٠٤) Ellis. *The International Legal Implications*: 4-10.

(١٠٥) Anthony M. Helm, ed. *The Law of War in the 21st Century: Weaponry and the Use of Force*. International Law Studies 82 (Newport, RI: Naval War College, 2006): 137-166.

(١٠٦) مصطفى سلامة حسين، **التأثير المتبادل بين التقدم العلمي والتكنولوجي والقانون الدولي** (القاهرة: دار النهضة العربية، ١٩٩٠): ٥٦–٧٨.

وأصبح هناك تأثيرات على بنية وتفاعلات العلاقات الدولية بشكل عام، أما الأول فهو الانتقال من فضاء قانوني مبني على أساس الجغرافيا إلى فضاء قانوني يحتوي في أحد أبعاده التحلل من الأساس الجغرافي والارتباط بالفضاء الإلكتروني؛ حيث ينتفي مفهوم الحدود بمعناها الجغرافي.

وترتب على هذا التحول ضرورة إعادة النظر في ثلاثة مفاهيم هي مفهوم السلطة القانونية ومفهوم التأثير والنفوذ ومفهوم الشرعية، وثانيًا: كما هي المتغيرات الداخلية والمتغيرات الخارجية في تفاعل الوحدات الدولية إلى درجة أصبح الاختصاص المحلي والاختصاص الدولي أمرًا ليس من اليسير البت فيه. وثالثًا: تجاوز الحدود القضائية ويشتمل على المزج ما بين الجرائم والفضاء الإلكتروني بكل أنواعها كتخريب الممتلكات والسرقة، وكانت الإباحية المخلة بالأخلاق وممارسة العنف سواء من خلال العنف اللفظي أو توظيف الفضاء الإلكتروني في ممارسة العنف المادي. ومن المجالات التي تأثرت بالثورة التكنولوجية ظهور الفضاء الإلكتروني، وتعرضه للهجمات وممارسة الأعمال العدائية، وحيث تمثل تلك الهجمات «الحرب الرخيصة» مقارنة بالأسلحة الأخرى، وأصبحت بذلك عنصرًا جاذبًا للدول والجماعات الإرهابية، ويناسب حالة الصراع بين أطراف متفاوتة في القوى.

ثانيًا: مبادئ القانون الدولي الإنساني والفضاء الإلكتروني

هناك مبادئ عامة أقرَّها القانون الدولي بشأن استخدام القوة في العلاقات الدولية. وعلى الرغم من أن القوة المقصودة هي القوة الصلبة، فإننا نحاول أن نجتهد في التوفيق بين إرادة المشرع الدولي وما فرضته الثورة التكنولوجية من تحديات. خاصة تلك التي تتعلق بالنزاعات المسلحة دولية الطابع أو غير الدولية، والتي تتميز بالطبيعة العرفية العامة والآمرة التي تسري في مواجهة جميع الأطراف المتحاربة، بغض النظر عن كونهم أطرافًا في الاتفاقيات الدولية المتضمنة لهذه المبادئ أو ليسوا كذلك. ومن هذه المبادئ التي يمكن الاسترشاد بها: مبدأ حق المتحاربين في استخدام وسائل القتال وأساليبه، وما يرتبط بها من

حظر استخدام الأسلحة التي تسبب آلامًا مفرطة، كذلك مبدأ التمييز بين المقاتلين والمدنيين وبين الأهداف العسكرية والمنشآت المدنية والمنشآت ذات الطبيعة الخطرة(١٠٧).

جاءت القاعدة العامة في القانون الدولي الإنساني الواردة في المادة ٣٥ من البروتوكول الإضافي الأول للعام ١٩٧٧ الملحق باتفاقيات جنيف الأربع للعام ١٩٤٩ لتنصَّ على أن «حقَّ أطراف أي نزاع مسلح في اختيار أساليب القتال ووسائله ليس حقًّا لا تقيده قيود»، و«المقصود بالأساليب هو طرق القتال. أمَّا الوسائل فهي الأسلحة والمعدات الموضوعة بتصرف المقاتلين أطراف النزاع»(١٠٨).

تطرق القانون الدولي الإنساني إلى معالجة استخدام الأسلحة من خلال ثلاثة مستويات، هي: المبدأ العام (أي تحديد مبادئ عامة بوصفها إطارًا شاملاً لضبط أي ثغرة قد يتم تغافلها في أي اتفاقية حاضرة أو مستقبلاً)، مثل ما عُرف بشرط مارتنز The Martens Clause الذي ورد في ديباجة اتفاقيتي لاهاي ١٨٩٩ و١٩٠٧. حيث نصَّت المادة الأولى منه على أن «يظل المدنيون والمقاتلون في الحالات التي لا ينص عليها هذا البروتوكول أو أي اتفاق دولي آخر تحت حماية وسلطان مبادئ القانون الدولي، كما استقرَّ بها العرف والمبادئ الإنسانية وما يمليه الضمير العام». أي أن الأطراف المتحاربة لا تستطيع من حيث المبدأ العام التذرع بعدم ورود نصٍّ صريح يتعلق بتحريم سلاح معين كي تعتبر أنه يحقُّ لها استخدامه بطريقة تتجاوز المبادئ العامة الإنسانية المشار إليها بالتحريم السلبي.

يعتبر القانون أي سلاح محرمًا استخدامه بطبيعته إذا نتجت عنه آثار عشوائية، وأن يُحدث أضرارًا جسيمة وآلامًا لا مبرر لها، وأن يُلحق بالبيئة الطبيعية أضرارًا بالغة واسعة الانتشار وطويلة الأمد. كذلك التحريم الإيجابي: أي تحريم أي سلاح ورد تحريمه بالاسم في إحدى الاتفاقيات ذات الصلة بالقانون؛ حيث يقسِّم القانون الأسلحة والذخائر إلى نوعين، الأول: أسلحة محرمة، أي محظور استخدامها لكونها وردت تسميتها بشكل واضح

(١٠٧) Mark Russell Shulman. *Legal Constraints on Information Warfare*. Occasional Paper no. 7 (Alabama: Air University. Center for Strategy and Technology, 1999), online e-book, www.au.af.mil/au/awc/awcgate/cst/csat7.pdf.

(١٠٨) إسماعيل عبد الرحمن، «الأسس الأولية للقانون الإنساني الدولي»، في **القانون الدولي الإنساني: دليل للتطبيق على الصعيد الوطني**، تقديم أحمد فتحي سرور (القاهرة: دار المستقبل العربي، ٢٠٠٣): ٢٠١-٣٤٠.

في معاهدات واتفاقيات دولية، أهمها تلك المتعلقة بحظر استخدام الأسلحة الكيماوية والبيولوجية والجرثومية والألغام المضادة للأفراد، والثاني: أسلحة مقيد استخدامها، أي مسموح استخدامها ولكن ضمن شروط معينة، وبشكل واضح من خلال نصوص وأحكام المعاهدات والاتفاقيات ذات الصلة.

هذه المعاهدات والاتفاقيات تكون ذات طابع دولي وتقع تحت مظلة القانون الاتفاقي، بمعنى أنها مُلزمة للأطراف التي انضمت لها. في حين أن القواعد والمبادئ ذات الطابع العرفي التي تتضمنها مصادر القانون الدولي الإنساني المختلفة ملزمة للجميع. أما الأسلحة المسموح باستخدامها أو التي لم يرد حظرها صراحة في أي اتفاقية أو إعلان أو معاهدة فيبقى استخدامها خاضعًا للمبادئ العامة. وتعرِّف المادة ٤٩ من البروتوكول الإضافي الأول الهجمات «بأنها تعني أعمال العنف ضد الخصم سواء أكان في حالة دفاع أم هجوم».

أقرَّت المادة ٥١ أربعة مبادئ عامة للتعامل مع المدنيين وقت النزاع المسلح. ولكن السؤال الذي يظل مطروحًا: هل يمكن اعتبار هجمات الكمبيوتر تقع خارج مدلول الهجوم لأنها لا تتضمن عنفًا؟ الإجابة: لا؛ وذلك لأن الهجمات المسلحة يمكن أن تتضمن هجمات الفضاء الإلكتروني التي يكون لها تداعيات مدنية. فالقانون الدولي الإنساني يمكن أن يطبَّق على هجمات الفضاء الإلكتروني إذا ما كانت تلك الهجمات تستهدف القتل أو التدمير، وفي ذلك اختلاف كبير عن طبيعة الهجمات التقليدية. وتأتي تلك الهجمات في طبيعة وطرق مختلفة، وتتم عبر وسيط مختلف لكي تتمكن هجمات الكمبيوتر من إصابة المطارات والبنية التحتية وأنظمة الاتصالات، بما يحمل تداعيات سياسية واقتصادية واجتماعية جسيمة تتعلق بالحياة المدنية بصفة عامة، وذلك مقارنة بالهجمات التقليدية بشكل يطرح وبوضوح التقدم في طرق الحرب ووسائلها[١٠٩].

من ثم فإن التركيز على نتائج تلك الهجمات التي يتم تنفيذها عبر الفضاء الإلكتروني يسهل علينا إمكانية أن تخضع تلك الهجمات للقانون الدولي الإنساني في مبادئه العامة،

(١٠٩) Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law* 37 (1998): 885-937.



وذلك إذا كانت عبارة عن جزء من الأعمال العدائية التقليدية. ومثلما كانت هناك أهداف محل الهجوم من العمليات العدائية التقليدية، فقد صارت هناك أهداف أخرى معرضة للخطر عن طريق استخدام هجمات الفضاء الإلكتروني بطريقة مباشرة أو غير مباشرة. وقد أوجد ذلك تداخلاً بين مفهوم العدوان ومفهوم الإرهاب سابقًا، كان مفهوم العدوان بشكله التقليدي يعني أنه «يقع ضد سلامة الأراضي والاستقلال السياسي من الدول، وأطرافها دول فقط». في حين أن الإرهاب جريمة تقع ضد سلامة الأشخاص وحقوقهم وحرياتهم الأساسية وأطرافها.

لكن هجمات الفضاء الإلكتروني أوجدت تداخلاً؛ فقد تقوم الدولة باستهداف الأشخاص وحرياتهم في صورة «إرهاب الدولة»، أو أن تتعرض الدول لمخاطر تهدد سلامتها وأمنها القومي وبنياتها الأساسية الحيوية.

في رأي اللجنة الدولية للصليب الأحمر أن اتفاقيات جنيف للعام ١٩٤٩ والبروتوكول الإضافي للعام ١٩٧٧ أخذت بعدًا أكثر اتساعًا في تناولها مفهوم «النزاع المسلح»؛ حيث تم تعريف النزاع المسلح بأنه «أي خلاف ينشب بين دولتين ويقود إلى تدخل القوة المسلحة»، حتى في حالة إنكار أحد الأطراف وجود حالة الحرب. وإنه بإعادة النظر فيما يتعلق بمبدأ «النسبية» الذي يتحدث عن وقوع أخطار تصيب الحياة المدنية وجرحى مدنيين ومنشآت مدنية أو التسبب في وقوع كل ما سبق، وحيث إن هجمات الكمبيوتر بإمكانها توسيع مدى ومجال الهجوم، فإن فرص استهدافه المنشآت ذات الطابع المدني تكون أكبر. وهذا ما يجعل من الظلم البين أن يتمَّ وصف ذلك على أنه يمثل ضعفًا في بنية وطبيعة هجوم الفضاء الإلكتروني، بقدر ما يجب أن يتمَّ اعتباره وببساطة تعبيرًا عن عملية توسُّع في وسائل الحرب المستخدمة وطرقها والتي تعتمد على التكنولوجيا المتقدمة. وهذا من شأنه أن يعني توسيع حجم الضرر الذي يمكن أن يلحق بالسكان المدنيين إذا ما تم التسليم بأن هجمات الإرهاب الإلكتروني تُعَدُّ نوعًا من أنواع الهجوم.

السؤال: إذًا ما الأهداف التي يمكن أن تستهدفها تلك الهجمات؟ بلا أدنى شك أو مبالغة فإنها يمكن أن تنحصر في ثلاثة أنواع؛ يشمل الأول منها: المحاربين والأهداف العسكرية،

الثاني: المدنيين والأهداف المدنية، الثالث: المنشآت التي تحظى بالحماية الخاصة أو التي تستحق الحماية.

فهناك من رأى أنه يمكن تطبيق القانون الدولي الإنساني على هذه الهجمات عن طريق القياس والاجتهاد في المقارنة. وهناك من رأى أن القانون الدولي الإنساني لا يمكن أن يُطبَّق على تلك الهجمات التي تحمل طبيعة خاصة، وتحتاج إلى نموذج قانوني جديد يتعامل معها وينظم استخدامها، والتي تصنَّف على أنها نوع من الأعمال التي تقوم بها دولة أو أكثر للإضرار برعايا دولة أخرى. ولا تتوقف الهجمات على عمليات القتل أو الخطف أو التدمير، وإنما تمتد إلى أي فعل من شأنه الإضرار بالأفراد بأي شكل كان. حيث لم يعد الأمر يقتصر على التصوُّر التقليدي للصراعات المسلحة، وإنما يمتد إلى شتى الأضرار التي تترتب على هذه الأفعال، وما تمثله من تهديد للأهمية الاستراتيجية للفضاء الإلكتروني(١١٠).

بذلك يمكن اعتبار الحرب الإلكترونية أحد أهم أشكال الصراعات التي يمكن أن تستند إلى مبادئ القانون الدولي الإنساني العام، والذي يجب ألا يقتصر فقط على الصراعات المسلحة المحدودة أو التقليدية. ففي المادة ٤٨ من البروتوكول الإضافي للعام ١٩٧٧ التي تعد الأساس الذي يمكن الاحتكام إليه فيما يتعلق بتوفير الحماية الدولية للمدنيين في أوقات الصراعات الدولية (هذه المادة تشمل جميع الصراعات العسكرية التي يمكن القياس عليها في حالة هجمات الفضاء الإلكتروني الموجَّه بشكل مباشر) لا يمكن التمييز بين ما هو عسكري وما هو مدني. فوفقًا للمادة ٤٩ التي تعرِّف الهجوم بأنه ممارسة العنف ضد الآخرين، يمكن أن يشمل ذلك كل أنواع العنف.

ثالثًا: هجمات أسلحة الفضاء الإلكتروني واستخدام القوة في العلاقات الدولية

أ– محددات استخدام القوة في العلاقات الدولية وشروطها:

أجاز القانون الدولي التقليدي استخدام القوة باعتبارها وسيلة مشروعة من وسائل فضِّ المنازعات الدولية، واقتصر دور القانون الدولي فقط على التنظيم القانوني للحرب،

(١١٠) James R. Hosek *et al., Attracting the Best: How the Military Competes for Information Technology Personnel* (Santa Monica, CA: RAND, 2004).



وكانت القوة مظهرًا من مظاهر السيادة الكاملة التي تلجأ إليها الدولة. وكانت النتائج الوخيمة الضارَّة للبشرية المنبثقة عن استخدام القوة في العلاقات الدولية دافعة إلى ضرورة الحدِّ من استخدامها، واعتبار ذلك عملاً غير مشروع دوليًّا. وذلك ابتداءً من اتفاقية لاهاي للسلام للعام ١٩٠٧، وميثاق بريان كيلوج للعام ١٩٢٨، ثم ميثاق الأمم المتحدة للعام ١٩٤٥ الذي أكد حظر استخدام القوة أو التهديد بها في العلاقات الدولية.

أجاز ميثاق الأمم المتحدة لكل دولة حقَّ الدفاع عن نفسها ضد عدوان خارجي يقع عليها، وفرض التزامات على الدول الأخرى لمساعدة الدولة المعتدَى عليها. وقد حددت الجمعية العامة للأمم المتحدة مفهوم العدوان والحالات التي ينطبق عليها، والتي بموجبها يحقُّ للدولة المعتدَى عليها أن تمارس حقَّها في مواجهة العدوان[١١١]. وأوجب ميثاق الأمم المتحدة على الدول أن تحلَّ منازعاتها بالطرق السلمية والامتناع في علاقاتها المتبادلة عن استخدام القوة أو التهديد باستخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة أو بأي طريقة أخرى تتعارض مع مقاصد الأمم المتحدة.

من هنا يتضح أن الميثاق لم يحظر اللجوء لاستخدام القوة فحسب، وإنما منع التهديد بها كذلك، ولم يُجِزْها إلا في حالة الدفاع الشرعي عن النفس ووفق ضوابط معينة. وقد كان ميثاق الأمم المتحدة قد أشار إلى حظر استخدام القوة في العلاقات الدولية؛ لأن لفظ مفهوم القوة المسلحة فقط شمل جميع أنواع القوة.

يرى الاتجاه الأول أن لفظ القوة الوارد في المادة ٢-٤ من الميثاق يجب تفسيره تفسيرًا ضيقًا، ومن ثم فإن اللجوء للقوة غير المسلحة لا يدخل ضمن تعريف تلك المادة لمفهوم القوة، وأن تلك الأشكال قد لا تدخل ضمن هذا الحظر. ويستند هؤلاء إلى النص في ديباجة الميثاق على «منع استخدام القوة المسلحة إلا للأغراض العسكرية»، وكذلك إلى المادة ٤٤ التي تنصُّ على أنه «إذا قرر مجلس الأمن استخدام القوة فإنه بذلك يكون قد قبل أن يطلب من عضو غير ممثل فيه تقديم القوة المسلحة».

---

(١١١) أحمد عبد الونيس علي شتا، **الدولة العاصية: دراسة في التعارض بين مواقف الدول والتزاماتها الدولية في الأمم المتحدة مع إشارة خاصة إلى إسرائيل وجنوب إفريقيا** (رسالة دكتوراه، جامعة القاهرة. كلية الاقتصاد والعلوم السياسية، ١٩٨٦): ٢٣٠-٤٥٠.

وحيث إن لفظ القوة الـوارد في الميثاق لا يشمل القوة المسلحة، فإن ما يسمى بالعدوان الاقتصادي أو الأيديولوجيا يدخل ضمن التدابير التي تمثل تهديدًا للسلم والأمن الدوليين، والتي تقع تحت طائلة المادة ٣٩ من الميثاق. ويرى أصحاب هذا الاتجاه أيضًا أن الأعمال التحضيرية للمادة ٢-٤ من الميثاق تؤكد أن مراد واضعي الميثاق من لفظ القوة هو القوة المسلحة؛ حيث تم استبعاد طلب البرازيل اعتبار إجراءات الضغط الاقتصادي ضمن الاستخدام غير المشروع للقوة.

يرى الاتجاه الثاني أن الضغوط الاقتصادية - بل كل الأعمال الانتقامية، سواء منها ما اتخذ شكل القوة المسلحة أو غيرها من الأعمال التي لا تصل إلى هذا الحد - تدخل في نطاق استعمال القوة التي جرَّمها الميثاق. كما أن نصوص الفصل السابع من الميثاق قد تحدثت عن وسائل الميثاق، وميزت بين الوسائل التي تقضي باستعمال القوة المسلحة وتلك التي لا تقضي باستعمالها. وأن المادة ٢-٤ حظرت الصور المحظورة للقوة، وبيَّنت أن تلك المواجهة ضد سلامة الأرض أو الاستقلال السياسي لأي دولة ولا تتفق مع مقاصد الأمم المتحدة، وليست القوة المسلحة وحدها هي التي من شأنها حدوث ذلك. بل إن ممارسة الضغوط الاقتصادية ضد دولة معينة قد تؤدي إلى نتائج مماثلة وبطريقة ملموسة، وأن المادة ٢-٤ من الميثاق استعملت لفظ القوة بدلاً من لفظ العنف، وذلك يفيد اشتمال الحظر على القوة المسلحة وسائر وسائل أساليب القهر الأخرى.

ب- مبدأ حظر استخدام القوة في العلاقات الدولية وأسلحة الفضاء الإلكتروني:

تقارِب هجمات الفضاء الإلكتروني الهجمات التقليدية في النتائج، لكنها تختلف عنها في الوسائل واستراتيجيات التنفيذ؛ حيث ينتج عن استخدامها خسائر مادية في الطرف الآخر، إلى جانب: شنِّ حرب نفسية، خلق حالة من شدة التنافس في الحصول على المعلومات، تطوير وامتلاك واستخدام ونقل الأسلحة الإلكترونية في الفضاء الإلكتروني. كما حدث تنوُّع في وسائل الحرب أو الصراع، وكذلك في الفاعلين في هذه الحرب من جماعات إرهابية أو شركات عاملة في تكنولوجيا المعلومات أو حكومات أو أفراد. وهذا من شأنه

أن يؤدي إلى خلق حرب مفتوحة، كما يفتح الباب إلى تطوير أساليب جديدة في الحرب مستقبلاً.

لهجمات الفضاء الإلكتروني دوافع متنوعة: تكنولوجية ومعلوماتية واجتماعية وثقافية وسياسية واقتصادية وعسكرية وغيرها. وتدفع أسلحة الفضاء الإلكتروني المخططين الحربيين وغيرهم إلى تنمية قدراتهم في استخدامها. بدلاً من المخاطرة بقصف شبكات الطاقة والسكك الحديدية وخطوط الهاتف من قِبل الطيران الحربي، أصبح بالإمكان استخدام الفضاء الإلكتروني في إحداث الأثر نفسه.

وعُني القانون الدولي الإنساني بالتفريق بين المقاتلين وغير المقاتلين بسبب: نمو عدد المقاتلين، تطوُّر أساليب الحرب، اللجوء إلى استخدام أساليب الحرب الاقتصادية. ومع أن الإسهام الحقيقي للقانون الدولي الإنساني يتضح في تحديد وتقييد التسلح وأبعاده الخاصة بالبعد الجغرافي: بتقليل المساحة التي يجوز فيها نشر واستخدام أنواع معينة من الأسلحة، وكذلك البعد المادي: بتقليل وسائل الحرب بفرض نوع من القيود على كمِّ الأسلحة المستخدمة ونوعها، وأيضًا ما يتعلق بالبعد العملي: بتحديد طرق استخدام هذه الأسلحة، والبعد الغائي: بفرض قيود على اختيار الأهداف التي توجَّه إليها الأسلحة؛ فإننا نجد أن تقييد التسليح يقلل من مخاطر نشوب الحرب. وساهم القانون الدولي الإنساني في حظر توسيع العمليات العسكرية إلى المناطق منزوعة السلاح والأماكن غير المدافَع عنها والأعيان المدنية والمناطق التي تحظى بالحماية. كما حظر استخدام الأسلحة الكيماوية والبيولوجية والحارقة، وكذلك فرض قيودًا على بعض طرق وأساليب القتال والهجمات العشوائية(١١٢).

القانون الدولي الإنساني هو ما يتم تطبيقه في حالة اندلاع الصراع المسلح. ويتضمن نوعين من القواعد: الأولى التي تحدُّ من قدرة الأطراف على استخدام وسائل الحرب وطرقها، والأخرى تتعلق بتلك القواعد التي تحمي الأشخاص والممتلكات في أوقات النزاع المسلح. وعلى الرغم من أن القانون الدولي الإنساني لم يحدد طبيعة النشاط العسكري، فإن

(١١٢) Daniel M. Vadnais, *Law of Armed Conflict and Information Warfare-How Does the Rule Regarding: Reprisals Apply to an Information Warfare Attack?,* (Alabama: Air Command and Staff College. The Research Department, 1997): 5-25.



ذلك لم يعنِ حرية استخدام القوة بدون قيود وقواعد. فقد فرض القانون حظرًا على أنواع معينة من الأسلحة، بالإضافة إلى أنها تتسبب في أضرار لا مبرر لها. وقد أقرَّت إحدى القواعد الأساسية للقانون الدولي حقَّ الأطراف في حالة نشوب الصراع المسلح في أن يختاروا وسائل القتال أو طرقها، ولكن هذا الاختيار غير مفتوح ومحدد وفق قواعد خاصة(١١٣).

يمكن أن يتسبب استخدام أسلحة الفضاء الإلكتروني في إحداث أضرار أو إصابات لا يمكن التحكم في نتائجها أو السيطرة عليها. إلى جانب ضعف القدرة التمييزية لها، وهو ما يدخل أسلحة الفضاء الإلكتروني وهجماتها ضمن الحظر. الذي تعامل معه القانون الدولي مع أسلحة الدمار الشامل. بالإضافة إلى خطورتها على البنية التحتية الكونية للمعلومات والتراث الإنساني المشترك. يرى فريق آخر اعتبار تلك الهجمات تقع ضمن الهجوم المسلح، خاصة أنها تنتج أضرارًا كتلك الأضرار التي يسببها الهجوم التقليدي واستخدام القوة التقليدية(١١٤).

يعزز هذا الموقف أن تعبير القوة الوارد ذكره في المادة ٢-٤ لم يأتِ مضافًا في ميثاق الأمم المتحدة، بما يجعل نصَّ المادة يتسع ليشمل جميع أنواع القوة غير الشرعية. كما أن المادة ٤١ من الميثاق أشارت إلى أن استخدام الاتصالات عامل ضغط لا يدخل ضمن القوة المسلحة.

ومن ثم فإن هناك من يرى أن ذلك يمكن أن يكون بداية لإمكانية خضوع ذلك الهجوم لقواعد القانون الدولي الإنساني، لاسيما وأنه قد فرض قواعد لاستخدام القوة في العلاقات الدولية ووضع شروطًا فيما عُرف بقانون الحرب، ووضع التمييز بين المدنيين والعسكريين وبين المنشآت المدنية والأخرى العسكرية، وحظر استخدام الهجمات التي تُنتج أضرارًا لا مبرر لها، وفرض اتخاذ الاحتياطات أثناء الهجوم.

---

(١١٣) عبد الصادق، **الإرهاب الإلكتروني: القوة في العلاقات الدولية**: ١٩٠-١٩٥.

(١١٤) Knut Dörmann, “Computer Network Attack and International Humanitarian Law”, *International Committee of the Red Cross*; https://www.icrc.org/eng/resources/documents/article/other/5p2alj.htm; Knut Dörmann, “Applicability of the Additional Protocols to Computer Network Attacks”, *International Committee of the Red Cross*, https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.



وجاء ذلك أيضًا في المادة ٥٧ من البروتوكول الإضافي الأول، الذي نصَّ على أن «الهجمات الانتقامية تُعَدُّ شكلاً من أشكال العدوان». وفرض القانون الدولي حماية خاصة للمنشآت التي تحتوي على مواد خطرة أو التي لها أهمية خاصة كمحطات الطاقة والسدود والمستشفيات.

من ثم فإن أي وسيلة من وسائل الحرب يمكن أن تتعرض للمنشآت الخاضعة للحماية وفق القانوني الدولي تُعَدُّ انتهاكًا للسلم والأمن الدوليين، وفق ما أقرَّه ميثاق الأمم المتحدة. فهجمات الفضاء الإلكتروني يمكن أن يتمَّ شنُّها من خلال إصابة نظم المعلومات الخاصة بالتحكم والسيطرة للمرافق الحيوية الكونية، بما قد يؤدي إلى إصابتها بالضرر، وربما يؤدي إلى تدميرها. وهناك رأي آخر يرى أنه إذا لم يتمّ اعتبار هجمات شبكات الكمبيوتر والفضاء الإلكتروني هجومًا مسلحًا وفق القانون الدولي، فإنه على الأقل يجب اعتبارها تمثل تهديدًا للأمن والسلم الدوليين الذي هو من مقاصد وروح ميثاق الأمم المتحدة.

المبحث الرابع

تطبيقات القانون الدولي الإنساني على استخدامات الأسلحة الإلكترونية

أولاً: مشروعية استخدام هجمات الأسلحة الإلكترونية في حالة النزاع المسلح

تحليل مشروعية الاعتداءات باستخدام الفضاء الإلكتروني من منظور القانون الإنساني، وما يثيره من قضايا قانونية أساسية، ولا يتضمن قانون الحرب أي قواعد صريحة بشأن الاعتداءات في الفضاء الإلكتروني؛ حيث لا تكون هذه الاعتداءات حركية، أي ليست اعتداءات «مسلحة» في حد ذاتها. وينطبق القانون الدولي الإنساني بالفعل بالنظر إلى هدفه الأساسي، وهو حماية المدنيين من ويلات الحرب، ويكون الهدف من الاعتداء على الفضاء الإلكتروني هو تعريض الأشخاص المحميين أو الممتلكات المحمية للخطر – أو المخاطرة بحدوث ذلك – ويصبح القانون الإنساني منطبقًا، وتندرج تلك الاعتداءات تحت قانون الحرب. ولكن يبقى تحدي تعريف «النزاع المسلح» عبر الفضاء الإلكتروني ومقدرة القانون الدولي الإنساني على تنظيم أساليب ووسائل الحرب الجديدة، والمثيرة للجدل من الناحية المفاهيمية، على حد سواء[١١٥].

وتحليل مدى مشروعية استخدام هجمات الفضاء الإلكتروني أو حرب المعلومات في النزاع المسلح أو في حالة الدفاع الشرعي عن النفس وفق الأطر القانونية الدولية الحالية. ويثير ذلك مدى إمكانية أن يكون لتلك المبادئ علاقة في حال تطبيقها على هجمات الفضاء الإلكتروني، تنتهي بنتيجة مفادها عدم شرعية استخدامها في حالة النزاع المسلح. وتتعلق المبررات النظرية والعملية بالتالي:

١– مبدأ «تقييد حقوق المتحاربين في استخدام أسلحة الحرب في النزاع»:

انطلاقًا من تغيُّر طبيعة الحرب ومداها ومجالها فإن القيود التي يجب أن توضع على المتحاربين أثناء النزاع المسلح يجب أن تتم زيادتها؛ تلافيًا للضرر الذي يمكن أن يصيب غير

---

(١١٥) Michael N. Schmitt, “Wired Warfare: Computer Network Attack and Jus in Bello”. *IRRC* 84, no. 846 (June 2002): 365-400, online e-article, https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf.

الهدف المقصود، سواء من الأشخاص أو المنشآت المدنية أو ما يمكن أن ينتج من خسائر عرضية. خاصة مع تزايد الترابط بين دول العالم من خلال شبكات الاتصال والمعلومات، وتدخُّل ذلك في عمل منشآت حيوية وبنية تحتية كونية يصبح من شأن إلحاق الضرر بها إحداث خسائر مدمرة للأمن الإنساني.

أي سلاح لم يتم ذكره في أي اتفاقية لا يعني بالضرورة إباحة استخدامه، ويُعَدُّ المثال الواضح للحظر الوقائي الوحيد هو ما ورد في البروتوكول الرابع لاتفاقية الأسلحة التقليدية لعام ١٩٨٠ الخاص بحظر استخدام أسلحة الليزر المعمية والذي أُلحق باتفاقية عام ١٩٩٥.

وهذا السلاح تمَّ تحريمُه بمجرد بدء التجارب عليه، وقبل وضعه موضع الاستخدام العسكري الفعلي. لكن هذا المثال لا يمكن تعميمه؛ لأن معظم التجارب على الأسلحة الجديدة تعتبر أسرارًا عسكرية، وبالتالي من النادر التعرُّف على آثار تلك الأسلحة. ومن ثم، يأخذ تحريم استخدام سلاح معين حيزًا من الجهد والوقت والنيات الحسنة، وهذا ما قد لا يتوافر، أو يتم التحقق من صحته.

تمَّ التركيز في اتفاقية جنيف للعام ١٩٤٩ على حماية الأشخاص في حالة الحرب، دون الإشارة إلى هجمات الفضاء الإلكتروني، ودون الإشارة إلى استخدام أسلحة معينة. وتناولت البروتوكولات الإضافية عددًا من طرق الحرب ووسائلها بصفة عامة. لذلك تعد البروتوكولات الإضافية أكثر ملاءمة لتقديم خريطة عمل للموقف من استخدام هجمات الفضاء الإلكتروني. وتمت الإشارة بشكل واضح في المادة ٣٦ من البروتوكول الإضافي الأول إلى تبني واضعي تلك المادة التطورات الحديثة في وسائل القتال وطرقه، والتي نصَّت على أن «يلتزم أي طرف سام متعاقد – عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب – بأن يتحقق مما إذا كان ذلك محظورًا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق (البروتوكول) أو أي قاعدة أخرى من قواعد القانون الدولي»[١١٦].

(١١٦) Dörmann, "Computer Network Attack and International Humanitarian Law".



أقرَّت بذلك تلك المادة حقيقة أن أي نشاط عسكري معين يرتبط بطرق الحرب لم يتم تنظيمه بشكل دقيق لا يعني ذلك أنه يمكن استخدامه بدون أي قواعد. ولذلك فإن الأشكال الحديثة لهجمات الفضاء الإلكتروني وحرب المعلومات – التي لم يتمّ تضمينها في استخدامات الأسلحة التقليدية في الاتفاقيات الدولية – ترتبط بالقانون الدولي الإنساني وتخضع له كأي سلاح جديد عندما يتمُّ استخدامه في النزاع المسلح. فإحدى القواعد الأساسية للقانون الدولي الإنساني تقرُّ بأن «حقَّ أطراف النزاع في اختيار وسائل القتال وطرقه ليس مطلقًا»، كما جاء في المادة ٣٥ فقرة ١ من البروتوكول الإضافي الأول.

يتمُّ توجيه هجمات الفضاء الإلكتروني للعدوِّ أو الخصم، وذلك بهدف تحقيق أضرار، وهذا ما يجعلها طريقة للحرب ووسيلة، لا سيما وأنها تتميز بقدرتها الفائقة على تعدي الحدود الدولية، سرعه تنفيذها، عدم القدرة على تحجيم آثارها، كذلك صعوبة تحديد حجم المسئولية القانونية للدولة، خاصة أنه قد يستخدمها أشخاص مدنيون خارج نطاق القوات المسلحة أو فاعلون من غير الدول.

٢– مبدأ «حظر الآلام التي لا مبرر لها»:

تعتمد البنية الأساسية الحرجة في الكثير من الدول في عملها على شبكات تكنولوجيا الاتصال والمعلومات، التي تتراوح ما بين الاتصالات إلى خدمات الطوارئ، ومن الصفقات المالية إلى العمليات العسكرية والخدمات الحكومية والتجارة الإلكترونية والاقتصاد الرقمي. ويعكس ذلك مدى الارتباط الشديد بين الطابع المدني للفضاء الإلكتروني وإمكانية تعرُّضه للخطر، بما يسبب أضرارًا اقتصادية وسياسية واجتماعية.

من ثم فإن استخدام هجمات الفضاء الإلكتروني من شأنه أن تنشأ عنه آلام مفرطة، بما يتنافى مع الاتفاقيات الدولية التي حظرت استخدام الأسلحة التي تسبب آلامًا لا مبرر لها. وبالرغم من عدم تحديد الفضاء الإلكتروني باعتباره مجالاً لذلك التحريم، فإننا يمكننا قياس ما ورد في تلك الاتفاقيات على ما يمكن أن ينتج عن استخدام الفضاء الإلكتروني لإصابة أي بنى تحتية حيوية، تشكل مصلحة للمجتمع الدولي قاطبة، ولا تختلف عن نتائج استخدام

القوة والعمل العسكري التقليدي. حيث إن هناك اختلافًا في الآليات العدائية، ولكنها تتشابه في الآثار والنتائج، عبر استخدام أسلحة الفضاء الإلكتروني المتنوعة.

٣- مبدأ «التمييز بين المقاتلين وغير المقاتلين وما بين المنشآت المدنية والعسكرية»:

أصبحت مبادئ التمييز تشهد توسعًا في تعيين الأهداف العسكرية التي كانت تُعَدُّ هي الأهداف المشروعة للحرب وفق القانون الدولي. ولكن عندما يتمُّ تطبيق ذلك على هجمات الفضاء الإلكتروني، فإن هناك تغيُّرًا في مجال الصراعات المسلحة وأهدافها. وقد حدث تداخل فيما بين الاستخدامات المدنية والعسكرية؛ حيث إن كلتيهما ترتبط عبر شبكة واحدة ووسيط واحد هو الفضاء الإلكتروني. كما أن طبيعة الاستخدام ليست ثابتة ومتحركة ومتداخلة، ومن ثم فإن هناك صعوبة في تحديد الأهداف العسكرية التي قد تكون هدفًا للحرب.

ظهر مفهوم حديث للحرب يواجه بتحدي تعريف الهدف العسكري؛ وذلك لأن طبيعة الحرب قد تغيَّرت بشكل كبير. ومن ثم فإن استخدام هجمات الفضاء الإلكتروني يمكن أن يوسِّع مجال الحرب ويعمل على نشر أسلحة الفضاء الإلكتروني، وذلك مقارنة بالقواعد الأخرى التقليدية التي تقيد انتشار الأسلحة التقليدية واستخدامها. وحدث تطور مماثل في أساليب القتال والحرب وجعلها متعدية الحدود والمكان والزمان، ولو كان ذلك خارج نطاق العمليات العسكرية. واقتضى هذا التطور وضع القواعد والأحكام التي تكفل حماية المدنيين والأعيان المدنية ضد أخطار الحروب وأضرارها، من خلال وضع القيود والضوابط التي يُستعان بها في التمييز بين الأهداف العسكرية والأعيان المدنية وبين المحاربين وغير المحاربين. ففي حرب الفضاء الإلكتروني تصبح مسألة التفريق بين من يقاتل أو من لا يقاتل صعبة؛ حيث لا يوجد أسرى أو جرحى، بل توجد مرافق وأنظمة لا تعمل، أو دمار ذاتي مِن دون تدخل مباشر كالقصف والتدمير التقليدي. ومن ثم فإن تحديد مفهوم «الهجوم» يشكل أهمية قصوى لمعرفة كيفية تطبيق القواعد الخاصة بمبدأ التمييز والقوانين التي تعطي الحماية الخاصة لأهداف ومنشآت معينة.

وتعرف المادة ٤٩ من البروتوكول الإضافي الأول (فقرة ١) الهجمات بأنها «أعمال العنف الهجومية والدفاعية ضد الخصم». وأشار البروتوكول الأول إلى تعريف «أعمال العنف» التي تتضمن استخدام القوة الطبيعية؛ لذلك شمل مفهوم «الهجمات» أشكالاً أخرى تتضمن الوسائل غير الطبيعية كـ: الحرب النفسية، الحرب السياسية، الحرب الاقتصادية.

وبناءً على فهم ذلك والتمييز بينه وبين غيره من المصطلحات، فإن هجمات الفضاء الإلكتروني التي تستخدم الفيروسات والدود والقنابل المنطقية والبريد المتطفل وشلّ الخدمة والبريد الدعائي وغيرها، تُعَدُّ نوعًا من أنواع الهجوم يمكن أن يسبب أضرارًا ملموسة للأشخاص أو لمنشآت حيوية يقف من ورائها برنامج كمبيوتر أو هجوم معلوماتي، ويمكن أن تصنَّف بوصفها نوعًا من أنواع العنف. وهذا النوع من الهجوم يدخل ضمن اختصاص القانون الدولي الإنساني. كما قد يشمل هجوم الفضاء الإلكتروني نوعًا من الحرب النفسية أو سرقة أسرار ونشر شائعات كاذبة أو تعطيل عمل مؤسسات المال والأعمال. ومن ثم فإنه إذا ما اعتبرنا ذلك يمثل هجومًا مسلحًا، فإنها ستخضع لما قرره البروتوكول الإضافي بشأن الهجوم، والذي أقرَّ في المواد: ٤٨، ٥١ (٢)، ٥٢ بالالتزام بالهجوم المباشر على الأهداف العسكرية وتجنُّب التعرُّض للمدنيين والأهداف المدنية.

٤- مبدأ «حظر الهجمات العشوائية»:

إن الهجمات العشوائية «هي التي من شأنها أن تصيب الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز». وأقرَّت المواد ٨-٥١-٥٧ من البروتوكول الإضافي الأول لاتفاقيات جنيف للعام ١٩٧٧ حظر الهجمات العشوائية التي لا توجَّه إلى هدف عسكري محدد، أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجَّه إلى هدف عسكري، أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه البروتوكول. ومن ثم فإن من شأنها أن تصيب في كل حالة كهذه الأهداف العسكرية



والأشخاص المدنيين أو الأعيان المدنية دون تمييز؛ حيث إن طبيعة تلك الهجمات لا تملك القدرة على التمييز بين ما هو مدني وما هو عسكري(١١٧).

جرى تأكيد حظر الهجمات العشوائية في المادة ٥١ (٤) من البروتوكول الإضافي الأول؛ حيث إن الهجمات العشوائية هي تلك الهجمات التي لا تستهدف هدفًا عسكريًّا محددًا، أو ذلك الهجوم الذي لا يمكن التحكم في آثاره أو التنبؤ بتداعياته. والمادة ٥١ (٤) و٥١ (٥) من البروتوكول الأول تعدِّد خمسة أنواع من الهجمات العشوائية، هي تلك التي:

١- لا توجَّه إلى هدف عسكري محدد.

٢- تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجَّه إلى هدف عسكري محدد.

٣- لا يمكن حصر آثارها على النحو الذي يتطلبه البروتوكول.

٤- تعالج عددًا من الأهداف العسكرية واضحة التباعد والتميُّز بعضها عن البعض الآخر والواقعة في منطقة حضرية، على أنها هدف عسكري واحد.

٥- تنتهك مبدأ التناسب بين الميزة العسكرية وخسائر المدنيين.

تبعد تلك القواعد في حال تطبيقها على هجمات الفضاء الإلكتروني، والتي ربما تمثل عملية استخدامها خطورة أكثر. وتبقى مسألة توجيه هجمات الفضاء الإلكتروني إلى أهداف محددة شيئًا غير متوقع أو يمكن التحكم فيه وفي نتائجه على الأهداف المدنية وغير المدنية كذلك؛ حيث تتميز تلك الهجمات بـ: اتساع مجالها، كارثية نتائجها، عشوائية الإصابة.

فمثلاً عندما يتم إطلاق هجوم من الفيروسات على أنظمة الكمبيوتر لدولة مستهدفة - مع بُعد تلك الهجمات عن الدول المحايدة أو الصديقة - فإن ذلك الهجوم سيوضح الترابط الكبير بين شبكات الكمبيوتر ذات البعد العسكري والأخرى ذات البعد المدني. ومن ثم فإن تلك الهجمات ستتصف بـ: العشوائية، صعوبة التحكم في نتائجها التي يجرِّمها القانون الدولي الإنساني. كما أقرَّ بذلك البروتوكول الإضافي الأول. وشمل الهدف العسكري:

---

(١١٧) «الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف، ١٩٧٧»، **اللجنة الدولية للصليب الأحمر**، https://www.icrc.org/ara/resources/documents/misc/5ntccf.htm.



المقاتلين، المنشآت، وسائل النقل العسكرية، المواقع العسكرية، المواقع ذات الأهمية التكتيكية. أما الهدف المدني فيشمل: المدنيين، المنشآت المدنية بجميع أشكالها، وسائل النقل المدنية.

كشفت الهجمات التي تعرضت لها إستونيا في إبريل – مايو من العام ٢٠٠٧ وإبان الحرب الجورجية – الروسية في أغسطس من العام ٢٠٠٨ عن أنها كانت غير تمييزية؛ حيث إنها وُجِّهت إلى خطوط الاتصالات عن طريق توجيه المئات من القنابل «الميجابيتات». وهذا الهجوم لم يتعرض للسكان فقط، بل إنه تسبب في توقف أرقام الطوارئ التي تُستخدم في استدعاء الإسعاف وخدمات المطافئ لما يزيد على ساعة، وهي التي تقع ضمن المنشآت المحمية وفق القانون الدولي.

٥– حماية الأهداف المدنية والمنشآت التي تحتوي على خطورة خاصة:

تشمل حماية: الأشخاص من التعرُّض لآثار النزاع المسلح، المنشآت المدنية، المنشآت ذات الطبيعة الخاصة التي تتعلق مثلاً بسير الاتصالات في العالم أو الأقمار الاصطناعية أو شبكات الإنترنت. ولا شكَّ أن هجمات الفضاء الإلكتروني ستوسع من مجال الأهداف الشرعية؛ وذلك لأنها ستتضمن هجومًا، مع تأثيرات غير متوقعة ضد الأهداف غير المستهدفة قانونًا. فالهجمات يمكن فقط أن يتم توجيهها إلى الأهداف العسكرية، وتلك الأهداف يجب أن تحمل صفات الهدف العسكري، الذي لا يتم الاعتماد على تحديده تبعًا لوسيلة الحرب المستخدمة.

المادة ٥٦ من البروتوكول الإضافي الأول الخاصة بحماية الأشغال الهندسية والمنشآت المحتوية على قوى خطرة، تقرُّ بأن «لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربية محلاً للهجوم، حتى ولو كانت أهدافًا عسكرية، إذا كان من شأن مثل هذا الهجوم أن يتسبب في انطلاق قوى خطرة ترتب خسائر فادحة بين السكان المدنيين»[١١٨].

(١١٨) **دراسات في القانون الدولي الإنساني**، تقديم مفيد شهاب (القاهرة: دار المستقبل العربي، ٢٠٠٠): ٣٤–٣٥.



«ولا يجوز تعريض الأهداف العسكرية الأخرى الواقعة عند هذه الأشغال الهندسية أو المنشآت أو على مقربة منها للهجوم إذا كان من شأن مثل هذا الهجوم أن يتسبب في انطلاق قوى خطرة من الأشغال الهندسية أو المنشآت ترتب خسائر فادحة بين السكان المدنيين». وتعتمد تلك المنشآت على أنظمة الكمبيوتر والشبكات في تشغيلها وعلى الفضاء الإلكتروني بصفه عامة، وسمح ذلك بإمكانية تعرُّضها لخطر وقف العمل باستخدام هجمات الفضاء الإلكتروني. ومن ثم فإن تعرُّض تلك المنشآت لتلك الأخطار يمثِّل انتهاكًا لما ورد في روح تلك المادة، وهو الحفاظ على تلك المنشآت من أن تكون عرضة لأي هجوم.

إن إصابة تلك المنشآت ستمثل انتهاكًا لحماية البيئة التي أقرَّتها المادة ٥٥ من البروتوكول الإضافي الأول التي أقرَّت بأن «تراعى أثناء القتال حماية البيئة الطبيعية من الأضرار البالغة واسعة الانتشار وطويلة الأمد. وتتضمن هذه الحماية: حظر استخدام أساليب أو وسائل القتال التي يُقصد بها أو يُتوقع منها أن تسبب مثل هذه الأضرار بالبيئة الطبيعية، ومن ثم تضرُّ بصحة أو بقاء السكان». وعندما تعتمد مصانع الكيماويات أو محطات الطاقة النووية على أنظمة الكمبيوتر فإن تعرُّضها سيمثل تلوثًا شديدًا للبيئة وللسكان المدنيين.

٦- حماية وسائل النقل التي يتم استخدامها من قِبل المدنيين:

كما كان للحرب التقليدية بنية تحتية يتم الاعتماد عليها، بالإضافة إلى ما نصَّ عليه قانون الحرب من حماية لوسائل النقل التي يستخدمها المدنيون كالبنية الأساسية للسكك الحديدية أو الحافلات، فكذلك الحال مع هجمات الفضاء الإلكتروني التي تعتمد على وسائل يُستخدم أغلبها في الشأن المدني ككابلات الاتصالات ومحطات البثِّ ووصلات الإنترنت، والتي يمكن اعتبارها من المنشآت المدنية وتجب حمايتها. بل إنها من المنشآت التي تتطلب حماية خاصة، كتلك التي تناولها القانون الدولي بشأن حماية المنشآت التي تحتوي على مواد خطرة.

كما أن القانون الدولي للبحار لعام ١٩٨٢ قد تناول حماية الكابلات البحرية التي يمرُّ بها ٩٥٪ من اتصالات المجتمع الدولي وشبكة الإنترنت، ففي الفرع الرابع من قانون البحار الذي اعتُمد في يونية ١٩٩٤، تنصُّ الفقرة (٣٧) منه على الآتي: «يجب أن يسهر المحاربون



على تجنب الإضرار بالكابلات وخطوط الأنابيب المركبة في قيعان البحار التي لا تعود بالفائدة على المحاربين وحدهم»[١١٩].

٧- الاحتياطات أثناء الهجوم وواجبات القادة في الميدان:

تعني أن المتحاربين أو أطراف النزاع يجب أن يتخذوا جميع الاحتياطات الممكنة عند تبني وسائل الهجوم وأساليبه، بل يجب تجنب إحداث الخسائر في أرواح المدنيين أو إلحاق الإصابة بهم أو الأضرار المدنية، وأن يمتنع الطرف المحارب أو يلغي أو يعلق أي قرار يتعلق بشنِّ هجوم قد يتم توقُّع نتائجه بصورة عرضية، أو أن يُحدث خسائر في أرواح المدنيين والأعيان المدنية، أو أن يُحدث خلطًا من هذه الخسائر والأضرار، وأن يتم توجيه إنذار مسبق في حالة الهجوم، وأن يكون الهدف العسكري ممكنًا بين عدة أهداف تفاديًا لإصابة المدنيين.

فرضت قابلية استخدام الفضاء الإلكتروني في مثل تلك الأنشطة العدائية بعض التعقيدات بخصوص الإجراء الاحتياطي الواجب اتخاذه في أثناء الهجوم، والذي ورد في المادة ٧٥ من البروتوكول الإضافي، والتي تتطلب أنه في حالة الهجوم يتمُّ الالتزام مبدئيًّا باتخاذ كل الإجراءات في شكل اختيار وسيلة وطريقة الهجوم والتي يمكن من خلالها: تجنُّب الأضرار التي قد تصيب المدنيين وتقليصها إلى أقل حدٍّ ممكن، إمكانية الحدِّ من الأضرار. وهذا ما يجعل هناك صعوبة في ممارسة ذلك الهجوم. كما أن تشابك شبكات الاتصالات والمعلومات يجعل من الصعوبة بمكان التمييز بين ما يُعَدُّ أنظمة مدنية وأخرى عسكرية، وبالتالي معرفة الأهداف العسكرية التي يكون استهدافها قانونيًّا، والأهداف المدنية التي يجب أن تبقى بعيدًا عن الهجوم إذا ما سلمنا – فرضًا – بمشروعية استخدام هجمات الفضاء الإلكتروني.

٨- حظر الانتقام والعدوان غير المباشر:

تتضمن أعمال الانتقام استخدام القوة المسلحة من أجل ممارسة أعمال الإكراه المخالفة في حدِّ ذاتها لقواعد القانون الدولي العام ضد دولة أخرى سبق أن ارتكبت عملاً

(١١٩) «دليل سان ريمو بشأن القانون الدولي المطبق في النزاعات المسلحة في البحار»، **المجلة الدولية للصليب الأحمر**، العدد ٣٠٩ (٣١ ديسمبر ١٩٩٥)، مقالة إلكترونية متاحة عبر الإنترنت، https://www.icrc.org/ara/resources/documents/misc/5qzknh.htm.

غير مشروع. ومن ثم فإن أعمال الانتقام إن كانت في حدِّ ذاتها غير مشروعة، فإنها قد تكون غير ذلك إذا كانت بهدف العمل على احترام الشرعية الدولية. وقد تكون تلك الأعمال ذات طابع عسكري وغير عسكري، كما أن مفهوم القوة التي تشكل عدوانًا قد تمَّ حصرُه فقط في استخدام القوة المسلحة، سواء كان مباشرًا أو غير مباشر.

لم يشر قرار التعريف إلى أن التهديد باستخدام القوة عمل من أعمال العدوان. كما لم تَرِدْ الإشارة إلى العدوان غير المباشر ولا العدوان الاقتصادي، فالعدوان غير المباشر قد ينصرف إلى جميع أنواع التدخل في شئون الدول الأخرى غير المشتملة على استخدام القوة المسلحة، بما يخالف المبادئ المعلنة في ميثاق الأمم المتحدة. وقد عرَّفت وثائق الأمم المتحدة عبر الجمعية العامة استخدام القوة بأنه «كل عدوان يُرتكب بصورة غير علنية، مهما كانت الأسلحة المستخدمة». وكذلك استعمال تعبير العدوان على بعض الصور الخطيرة لاستخدام القوة المسلحة بطريقة غير مباشرة؛ إذ نصَّت المادة ٣-٧ على أنه «يُعتبر من قبيل أعمال العدوان قيام الدول بإرسال عصابات أو جماعات مسلحة أو قوات غير نظامية أو مرتزقة تقوم ضد دولة أخرى بعمل من أعمال القوة المسلحة يكون على درجة الخطورة نفسها التي ورد ذكرها أو إشراك الدولة بدور ملموس في ذلك».

٩- مبدأ «المشاركة المباشرة في الأعمال العدائية»:

حددت المادة ٥٢ فقرة ٣ الظروف والشروط التي يفقد فيها المدني صفته المدنية ليدخل ضمن قانون الحرب باعتباره مقاتلاً. وتُعَدُّ حماية الصفة المدنية ذات أهمية خاصة؛ لأن من شأنها المساعدة في: الحدِّ من إلحاق الأضرار بالمدنيين، جعل الأهداف العسكرية مباشرة للهجوم. كما عرَّفت المادة ٥٠ الأشخاص المدنيين والسكان المدنيين، ولكن هذه المادة قد لا تجد مجالاً للتطبيق؛ وذلك لصعوبة الفصل بين ما إذا كان الفرد مدنيًّا أو عسكريًّا. فقد يمتلك الفرد خبرة بالكمبيوتر، وقد يشارك في الهجوم، ولكنه لا يحمل صفة عسكرية رسمية تابعة للدولة. وكذلك فقد يسهم بعض الخارجين على نطاق دولة ما في دعم موقفها إزاء دولة خصم. وهذا ما قد يساعد على فقد ذلك المدني صفته المدنية والحماية من الهجوم؛ وذلك باعتبارها مشاركة مباشرة من المدنيين في الهجوم.

هذا ما يتطلب معرفة مَنْ المتسبب في الضرر أو مَنْ استخدم هجمات الفضاء الإلكتروني باعتبارها شكلاً من أشكال «التطبيق المباشر للتدمير الإلكتروني بدافع تحقيق هدف عسكري». وقد أجمع عدد من الفقهاء على أن استخدام الوسائل الإلكترونية وسيلة لهجمات شبكة الكمبيوتر يمكن اعتباره مشاركة مباشرة في الأعمال العدائية. وهناك من رأى أن «استخدام هجمات الفضاء الإلكتروني في الأعمال العدائية لا يُعَدُّ مشاركة مباشرة في القتال إلا إذا ما نتج عنها الموت أو جرحى أو ضرر طبيعي». وهناك رأي آخر مفاده أنه لكي يتم اعتبار هجمات الفضاء الإلكتروني مشاركة مباشرة في القتال يجب أن تتوافر لها صفة التعمد. وهناك من رأى أن ذلك يخضع لطبيعة الموقف. ومسألة استخدام أسلحة الفضاء الإلكتروني يمكن أن تضرَّ بمصالح المجتمع الدولي، بما يجعل الإنسانية هي محل الاعتداء، وخاصة عند استخدام أنظمة التسلح ووسائل الاتصالات ووسائل المواصلات وطرقها والشبكات الإلكترونية في العمليات العسكرية، وتُعَدُّ حالة مشاركة مباشرة في الأعمال العدائية.

١٠- تهديد الجنس البشري:

استطاعت عقدة الصناعة الحربية أن تجعل البحث العلمي رهن إشارة الحرب، من أجل ضمان كفاءات الهدم المتبادل. كما أنه بواسطة تطوُّر المعلوماتية والتقنية الحيوية استطاعت علوم الحياة في الوقت نفسه أن تهدد النوع البشري، ليس كما كان بواسطة الإشعاع الذري وإنما عن طريق التلقيح السياسي. وعليه، فإن مراقبة مصادر الحياة وضبطها هي أصل بقاء الفرد، حين يصبح التهديد لا يهمُّ مجموعة بشرية بعينها وإنما النوع البشري برمته.

أصبحت المعلومة تشكل البعد الثالث للمادة بعد الكتلة والطاقة، ودخلت تكنولوجيا الاتصال والمعلومات مجالات البنية التحتية الكونية للمعلومات مثل: محطات الطاقة والمياه والسدود والمحطات النووية التي أصبحت ماسَّة ببقاء الإنسان ومعيشته. ومن ثم فإن تعرُّضها للتهديد لا يعني إلا إنتاج أنواع جديدة من الهدم لتطوير سلسلة من الحوادث الإرادية تضرُّ بمصلحة الإنسان وبقائه؛ حيث يتمُّ التعرُّضُ لحرب المعلومات والفضاء الإلكتروني. وبالطريقة نفسها يمكن للمعلومة المتوافرة أو غير المتوافرة ألا تكون سرية، ما دام كل هجوم



أو حادثة متساوية من حيث الوقوع[١٢٠]. وهذا ما يتسبب في إحداث أضرار بالغة للمجتمع الدولي أو التسبب في خسائر اقتصادية وانعكاس ذلك على أمن المجتمع الدولي.

١١- حماية المنشآت ذات الطبيعة الخاصة:

إن القانون الدولي الإنساني أقرَّ بوجوب حماية المنشآت ذات الحماية الخاصة، كمحطات الطاقة والمنشآت التي تحتوي على مواد خطرة أو المناطق الأثرية. ولقد أحدثت الثورة التكنولوجية تغيُّرًا في شأن اعتماد عدد من البنى التحتية الحيوية على الكمبيوتر والتحكم المركزي من خلاله. وفرض القانون الدولي الإنساني حماية للمنشآت المدنية التي تحتوي على خطورة خاصة بالمفاعلات النووية أو مستودعات المواد الكيماوية، والتي تعمل هجمات الفضاء الإلكتروني على إصابة تلك المنشآت، بما يتسبب في كوارث بيئية وإنسانية، مثل: المطارات أو خطوط السكك الحديدية أو محطات الطاقة وأنظمة الاتصالات والمصانع، التي قد تحمل استخدامين أحدهما مدني والآخر عسكري. فقد تُستخدم - مثلا - الأقمار الصناعية مثل إنتل سات Intelsat أو أورو سات Eurosat أو عرب سات Arabsat، وتنتقل من الاستخدام المدني إلى الطابع العسكري، وهذا يتوقف على ما إذا كان ذلك الهدف يحمل طابعًا عسكريًّا ينفي عنه الطابع المدني، ومن ثم يتم سحب الحماية المدنية القانونية. وكذلك يتوقف على طبيعة الصراع، فقد يستخدم المجال الجوي في عملية الدعم العسكري، ولكنه لا يحمل طبيعة عسكرية خالصة.

١٢- الفئات التي لا تتمتع بوضع أسرى الحرب:

أما بالنسبة إلى المشاركين في عملية الهجمات عبر الفضاء الإلكتروني فقد لا يتم اعتبارهم مدنيين - على الرغم من نفي صفة العسكرية عنهم - لأنهم يكونون أقرب إلى توصيف الجواسيس أو المرتزقة والذين لا يعاملهم القانون الدولي معاملة الأسرى، وهم: أولاً الجواسيس، وهم من يلجئون سرًّا إلى بعض مظاهر الخداع بجمع المعلومات العسكرية في الأراضي الخاضعة لسيطرة العدو. ويشترط في الجاسوس ألا يكون مرتديًا للزي العسكري

(١٢٠) بول فيريليو، «القنبلة المعلوماتية»، ترجمة عادل حدجامي، وسعيد توبير، **مجلة فكر ونقد**، العدد ٢٩ (٢٠٠٦)، مقالة إلكترونية متاحة عبر الإنترنت، http://www.fikrwanakd.aljabriabed.net/n29_14hajjami.%282%29.htm.



للقوات المسلحة التي ينتمي إليها. كما لا تتم معاملة الجاسوس بوصفه أسير حرب وفق المادة ٤٦ من البروتوكول الإضافي الأول لعام ١٩٧٧.

أما الفئة الثانية فهم المرتزقة وهم من جنسية مختلفة عن جنسية الدولة التي يتدخلون فيها. وقد تطرقت لهذه الفئة المادة ٤٧ من البروتوكول الأول للعام ١٩٧٧ الملحق باتفاقيات جنيف للعام ١٩٤٩؛ حيث لا يحقُّ للمرتزقة التمتُّع بوضع الأسير أو المقاتل؛ نظرًا لأنهم: من يجري تجنيدهم خصيصًا مرحليًّا أو في الخارج للمشاركة في القتال في النزاع المسلح، يشاركون فعلاً في الأعمال العدائية، ليسوا من رعايا طرف في النزاع، ليسوا أعضاء في القوات المسلحة لأحد أطراف النزاع، ليسوا موفدين رسميين. ومن ثم فإن المشاركين في هجمات الفضاء الإلكتروني يمكن اعتبارهم يخضعون لهذا التوصيف القانوني.

١٣- مبدأ «الحياد في القانون الدولي»:

إن استخدام الفضاء الإلكتروني لشنِّ هجمات يمثل انتهاكًا لمبدأ الحياد في القانون الدولي؛ حيث إن الفضاء الإلكتروني يمرُّ عبر حدود العديد من الدول، ومن ثم فإن الطابع الدولي للفضاء الإلكتروني يجعل أيًّا من أطراف النظام الدولي معرضين للإصابة من جراء شنِّ تلك الهجمات. كما أنه إذا تمَّ شنُّ تلك الهجمات فإنها تمرُّ عبر دولة ثالثة أو أكثر غير متورطة في الصراع، وعلى الرغم من عدم مسئوليتها القانونية فإنها قد تصبح متورطة في تلك الهجمات، وهذا ما يُعَدُّ انتهاكًا للقانون الدولي الإنساني واتفاقية جنيف؛ حيث جاء فيها «إن الدول والأطراف المشاركة في النزاع تمتنع عن تحريك القوات أو إرسال مستلزمات الحرب أو الإمدادات عن طريق أراضي الطرف المحايد».

يتحرك الفضاء الإلكتروني عبر شبكات الاتصال والمعلومات العابرة للحدود وبالتالي فإنها تمرُّ بدول محايدة. ويمكن أن تحمل أسلحة خاصة تختلف في التكتيك وطرق العمل، ولكنها تدخل ضمن تعريف الأسلحة باعتبارها «أدوات للقتل أو إلحاق الضرر أو التسبب في وجود جرحى أو تدمير ممتلكات للخصم». ومن ثم فإن الدول المحايدة تمتنع عن نقل أسلحة الفضاء الإلكتروني عبر شبكات الاتصال والمعلومات التي تمرُّ عبر أراضيها. فأسلحة

الفضاء الإلكتروني يمكن أن تُلحق الضرر بالمدنيين والمنشآت المدنية؛ ولذلك فإن هجوم الفضاء الإلكتروني مثل غيره من أنواع الهجوم التقليدي، وقد يمرُّ ذلك الهجوم عبر دولة أخرى وقد لا تشعر به.

١٤- مبدأ «مارتنز»:

تم إدراج هذا الشرط في الفقرة ٢ من المادة الأولى من البروتوكول الإضافي الأول للعام ١٩٧٧ التي تنصُّ على أن «يظل المدنيون والمقاتلون في الحالات التي لا يُنص عليها في هذا الملحق (البروتوكول) أو أي اتفاق دولي آخر تحت حماية وسلطان مبادئ القانون الدولي، كما استقرَّ بها العرف ومبادئ الإنسانية وما يمليه الضمير العام». ويُطلق على هذا الشرط اسم المبدأ البديل؛ باعتبار أنه يطبَّق عند عدم وجود نصٍّ يحكم علاقة الشخص أو الأشخاص المعنيين بخصوص مسألة أو حالة لم يَرِدْ بشأنها نص صريح. لذلك تقضي اتفاقيات جنيف بضرورة معالجة الحالات التي لم يُنصّ عليها «على هدى المبادئ العامة الواردة في تلك الاتفاقيات في المادتين ٤٥ و٤٦ من الاتفاقين الأول والثاني».

١٥- مبدأ «إن المزايا الحربية لا يمكن أن تزيل حقوق الفئات المحمية»:

حيث لا يجوز أن يترتب على الميزة العسكرية التي يرمي أي طرف من أطراف النزاع إلى تحقيقها الاعتداء على الحقوق المقررة للفئات المحمية؛ إذ يجب أن يتمَّ اتخاذُ الاحتياطات الواجبة لتجنيب المدنيين والأشياء المدنية إلى أقصى قدر ممكن ويلات النزاع المسلح. لذلك يحظر الهجمات العشوائية أو غير المميزة. ومثال ذلك: الهجوم الذي يرتب آثارًا جانبية جسيمة على السكان المدنيين والأهداف المدنية، بما لا يتناسب مع الفائدة العسكرية المتوقعة (م: ٥١، ٥٢، ٥٧) من البروتوكول الإضافي الأول.

١٦- حماية التراث الإنساني:

فقد نصَّت المادة ٥٣ من البروتوكول الإضافي الأول على حماية الأعيان الثقافية وأماكن العبادة في إطار أحكام اتفاقية لاهاي المتعلقة بحماية الأعيان الثقافية في حالة النزاع المسلح الصادرة في ١٤ من مايو للعام ١٩٥٤ والبروتوكول الثاني للاتفاقية المبرم في

لاهاي في ٢٦ من مارس للعام ١٩٩٩، وأحكام المواثيق الدولية الأخرى الخاصة. فإذا ما طبقنا نصَّ هذه المادة على الفضاء الإلكتروني فسنجده يحتوي على الأرشيفات الإلكترونية الوطنية والثقافية والتاريخية للدول، بما يشكل الحفاظ على الذاكرة الجمعية للدول والتراث الإنساني المشترك. ومن ثم فإن هجمات الفضاء الإلكتروني يمكن أن تخضع لهذه المادة. وبخاصة مع تحول الفضاء الإلكتروني إلى مرفق عالمي.

ثانيًا: مشروعية استخدام هجمات الفضاء الإلكتروني في حالة الدفاع الشرعي

أ – الدفاع الشرعي ومحددات استخدامه في القانون الدولي الإنساني:

توجد في ميثاق الأمم المتحدة قواعد قانونية تتعلق بحقِّ الدفاع الشرعي كونه حقًّا مشروعًا لكل معتدَى عليه عندما يقع عليه فعل الاعتداء، والذي يُعَدُّ جريمة على النفس أو المال. ونظمت كل القوانين الداخلية وبيّنت نشوء هذا الحقِّ واستعماله، والمادة ٥١ من ميثاق الأمم المتحدة نصّت على حق الدفاع الشرعي والتي جاء فيها: «ليس في هذا الميثاق ما يُضعف أو ينقص الحق الطبيعي للدول فرادى أو جماعات في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء هذه الهيئة، وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين»، وحتى عصبة الأمم اعترفت بهذا الحق. ونصّ بروتوكول جنيف للعام ١٩٢٤ على هذا الحق في المادة ٢ منه والتي جاء فيها «أن الدول الموقعة قد اتفقت على أنها سوف لا تلجأ للحرب وسيلةً لفضِّ النزاعات بأي حال إلا في حالة مقاومة العدوان».

لاستعمال حقِّ الدفاع الشرعي شروط في القانون الدولي؛ حيث إن الردَّ يجب أن يتقيّد بشرطين: الأول، أن تكون القوة المبذولة للردِّ موجهة إلى مصدر الاعتداء، فلا يجوز أن يكون المعتدي دولة وأن يوجَّه الردُّ لدولة أخرى. وعندما تمارَس هذه الحالة فإنها عدوان. والثاني، أن تكون القوة المبذولة للردِّ متناسبة مع العدوان، وفي حدود القدر الضروري لردِّ العدوان وإيقافه عند حدِّه. وأجاز القانون الدولي فعل الدفاع الذي يمكن أن يمارَس من قِبل

الغير على مصدر الاعتداء، شريطة أن يكون قرار التدخل حصريًّا لمجلس الأمن، وهذا ما نصّ عليه في مواد الميثاق ٣٩–٤٠–٤١–٤٢[١٢١].

حددت المادة ٥١ الإطار المنظم لكيفية الدفاع الشرعي والذي يمكن أن يتمَّ في شكل هجمات واضحة يتمُّ تصنيفُها على أنها هجوم مسلح. وجاءت هجمات الفضاء الإلكتروني أو حرب المعلومات لكي يتمَّ شنُّها على نطاق واسع. وأصبح غير كافٍ تصنيفها هجومًا مسلحًا وفق القانون الدولي التقليدي. ومن ثم لا تخضع لسلطة قانون الاتّفاقيات الدولية أو القانون الدولي العام أو القانون الجنائي العرفي.

كما أن ميثاق الأمم المتحدة يركز على مسألة تنظيم استخدام القوة فيما بين الدول وفق المادة ٢–٤ التي وضعت شروط التزام استخدام هذه القوة ونطاقها. وعند النظر إلى الهجمات التي يتمُّ شنُّها في الفضاء الإلكتروني وفق ما جاء في نصِّ المادة ٥١ فإنه يبقى تساؤل حول إذا ما كان يمكن تصنيف تلك الهجمات باعتبارها تخضع للتصنيف الخاص بالهجوم المسلح. ولكن عند التركيز على الوسائل المستخدمة في هجوم حرب المعلومات والإرهاب الإلكتروني فإنه يمكن القول إنها تضاهي ما يتم استخدامه في الحروب التقليدية في آثارها وتداعياتها، كما ينتج عنها قدر من القنابل والأسلحة والقصف والعدوان وغيرها من مظاهر استخدام القوة داخل الفضاء الإلكتروني، والذي يكون له تأثير مماثل لتأثير الهجمات التقليدية[١٢٢].

أكد ميثاق الأمم المتحدة تحريم استخدام القوة المسلحة أو التهديد باستخدامها ضد السلامة الإقليمية أو الاستقلال السياسي للدول الأعضاء في الأمم المتحدة، وذلك مع وجود حالات الضرورة التي حرص القانون الدولي من خلالها على تحجيم الحرب ووضع قيود عليها إذا ما وقعت. وأورد ميثاق الأمم المتحدة استثناءات لحالة الاستخدام المشروع للقوة في القانون الدولي، وهي حالات: الدفاع النفسي والجماعي الذي تضمنته المادة ٥١ من

---

(١٢١) **القانون الدولي الإنساني: دليل للتطبيق على الصعيد الوطني**، تقديم أحمد فتحي سرور (القاهرة: دار المستقبل العربي، ٢٠٠٣): ٣٢٠–٣٢١.

(١٢٢) Dimitrios Delibasis, “State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century”, *Peace Conflict and Development,* no. 8 (Feb 2006).

ميثاق الأمم المتحدة، حق تقرير المصير، حروب التحرير، العمليات الحربية التي يقوم بها المجتمع الدولي التي يقرُّها مجلس الأمن التابع للأمم المتحدة وفق أحكام الفصل السابع.

كلُّ ذلك وفق الضوابط والشروط التي وضعها الميثاق لتنظيم القوة كما ورد في المادة ٢٠، ويفرض مجموعة من الشروط الموضوعية التي تتمثل في: ضرورة وقوع عدوان مسلح، بما يجعل استخدام القوة في إطار الدفاع الشرعي عن النفس أمرًا مشروعًا متفقًا وصحيح القانون ومتناسبًا ما بين العدوان واستخدام القوة دفاعًا عن هذا العدوان. ومن ثم فإن ذلك يستهدف الحدَّ من استخدام القوة بوصفها عملاً ثأريًّا أو انتقاميًّا يكون غير مشروع ومرتبًّا للمسئولية الدولية في حق من أقدم عليه. أما الشروط الإجرائية فتتضمن أن تقوم الدولة التي تعرضت للعدوان بإبلاغ مجلس الأمن بوقوع العدوان وطبيعة ما اتخذته من إجراءات في مواجهته... مع حقها في الدفاع عن نفسها. ويتدخل مجلس الأمن ويباشر صلاحياته المخولة له حسبما تقضي به أحكام الميثاق[١٢٣].

أصبح المجتمع الدولي أمام نمط جديد من الحرب يحمل أساليب جديدة وهجومًا غير تقليدي في بيئة غير تقليدية ولها تداعيات غير محسوبة، وإذا ما نجحت فإنها تصيب المنشآت المدنية وتبثُّ الرعب والخوف وتؤثر على الاستقرار السياسي داخل الدول وعلى المجتمع الدولي قاطبة. ففي أحد السيناريوهات فإن هجمات الفضاء الإلكتروني قد تتمُّ من خلال الدخول إلى شبكات المعلومات بشكل غير شرعي، وبما يؤثر على عمل البنية التحتية الكونية للمعلومات، وما يكون له من تأثير على الدول فرادى وعلى المجتمع الدولي ككل، والذي أصبح يعتمد بشكل متزايد على تلك الشبكات الدولية باعتبارها مسهلات لتقديم الخدمات التي تتعلق بنمط الحياة المعاصر.

هذه الشبكات إن أصابها الضرر فإنها تهدد بوقوع خسائر وأضرار يقف خلفها دولة أو فاعل من غير الدول في مواجهة دولة أو أطراف من غير الدول، ويكون من آثار ذلك: بروز عمليات دفاع شرعي تأتي في مضمونها مع الحقِّ الذي أقرَّه القانون الدولي. إلا أن ظروف استخدام هذا الحقِّ وشروطه الموضوعة في ميثاق الأمم المتحدة أصبحت غير ملائمة

(١٢٣) شتا، **الدولة العاصية**: ٢٠٠–٣٥٠.



لممارسته داخل بيئة جديدة وتحديات جديدة يفرضها استخدام القوة في الفضاء الإلكتروني للدفاع الشرعي. كما يفرض تحديات تتعلق بإجراءات الوقاية والحماية ضد التعرُّض لمثل تلك الهجمات. ومن ثم فإن أفعال الدفاع الشرعي قد لا تأتي في شكل القيام بهجوم مسلح تقليدي، بل قد تتخذ أشكالاً أخرى لها تأثيراتها وتداعياتها على الفضاء الإلكتروني بوصفه مجالاً واحدًا تسبح به جميع المصالح والخدمات والتواصل العالمي، ويشكل أهمية استراتيجية للمجتمع الدولي، وينتج عن تعرُّضه لمسألة الدفاع والهجوم بلا شك تأثير على وظيفته وطبيعة دوره ومستقبله ويمسُّ أهميته للمجتمع الدولي.

ثار جدل واسع حول طبيعة الأعمال الهجومية والدفاعية التي يمكن أن تحدث في الفضاء الإلكتروني، والذي أصبح يرتبط بالاستراتيجية العسكرية من خلال القدرة على شنِّ طرق إنكار الخدمة أو الخداع أو التدمير أو الاستغلال، وهذا ما يفرض تحديات فيما يتعلق بمفهوم «العدوان»، وهو الذي يعني استخدام القوة المسلحة من قِبل دولة ضد السيادة أو الوحدة الإقليمية أو الاستقلال السياسي لدولة أخرى، أو بأي طريقة أخرى لا تتفق مع ميثاق الأمم المتحدة. وحتى يصبح العدوان جريمة بالمعنى القانوني الفعلي يجب أن تتوافر وتتحقق أركانها الأربعة وهي: الركن الشرعي، الركن المادي، الركن المعنوي، الركن الدولي.

يمكن أن تشنَّ الدول العدوان من خلال الفضاء الإلكتروني أو بمهاجمة نظم الاتصالات، أو قطع خدمة الإنترنت عن الدول الأعداء، أو استخدامه في الدعاية وشنِّ الحرب النفسية والتجسس والقرصنة وتدمير قواعد البيانات الخاصة بمنشآت مدنية، وبما يقارب حالة القصف الجوي التقليدي. ولكن ذلك يتمُّ عن طريق قصف فيروسات وهجمات داخل الفضاء الإلكتروني، أو التحريض على العنف داخل دولة معينة مستفيدة من الطابع الدولي للفضاء الإلكتروني. ويقابل ذلك صعوبات فيما يتعلق بقدرة الدول على الوصول إلى مرتكب الهجوم عبر الفضاء الإلكتروني، انتهاك مفهوم السيادة للدول الأخرى، القدرة على التمييز في حالة شنِّ الهجمات، كيفية تحصين الدولة في مواجهة خطر التعرُّض لها[١٢٤].

(١٢٤) Geoffrey S. DeWeese, “Anticipatory and Preemptive Self-defense in Cyberspace: the Challenge of Imminence”, in the *7th International Conference on Cyber Conflict Proceedings 2015,* edited by M. Maybaum, A.M. Osula and L. Lindström (n.p.: NATO Cooperative Cyber Defence Centre of Excellence, 2015), online e-book, https://ccdcoe.org/cycon/2015/proceedings/06_deweese.pdf.



هناك خطر تصاعد الهجمات عبر الفضاء الإلكتروني بالتزامن مع النمو ذاته فيما يتعلق بأسلحة الدمار الشامل. كما أن هناك دولاً عدة تعمل على نمو قدراتها في مجال حرب المعلومات وأسلحة الفضاء الإلكتروني. وأخذت هجمات الكمبيوتر والإرهاب الإلكتروني Cyber Attacks المزيد من الاهتمام إلى الحدِّ الذي وضعته الدول في إطار استراتيجيتها العسكرية، وما يثيره ذلك من تساؤلات حول حدود استخدام القوة في الفضاءِ الإلكتروني للردِّ على الهجمات في إطار الدفاع الشرعي أو في استخدامها باعتبارها نمطًا من أنماط استخدام القوة في العلاقات الدولية أو فيما يتعلق بالهجمات الوقائية؛ حيث فرضت هواجس التعرُّض للخطر في أي وقت انتهاج شتى الطرق للحماية، والتي تأخذ شكلا وقائيًّا أو استباقيًّا على مصدر التهديد المحتمل، أو العمل على تقوية نظم الحماية والمنعة ضد التعرُّض لمثل تلك الهجمات.

ب- محددات الدفاع الشرعي في حالة التعرُّض لهجمات الأسلحة الإلكترونية:

إن اندفاع دولة في الهجوم على دولة أخرى يمكن أن يدفع الدولة المعتدَى عليها للردِّ بهجمات مضادة دفاعًا عن النفس. وتلك الهجمات لم يتمّ تحديدها قانونًا في حق الدفاع الشرعي عن النفس. كما يواجَه الهجوم في الفضاء الإلكتروني بتحديات تتعلق بخصائص هذا الهجوم، الذي يتميز بأن المهاجمين يتسببون في سلسلة من الأضرار عن طريق الدخول إلى نظم المعلومات. وطبيعة تلك الهجمات تجعل من الصعوبة بمكان – إن لم يكن مستحيلاً – تحديد مركز الهجوم المباشر، بما يؤثر على فاعلية الردِّ الدفاعي. ولا توجد دولة يمكنها أن تصل إلى درجة عالية من المنعة ضد تلك الهجمات.

أما التحدي الثاني فيتعلق بإمكانية التعامل مع أي قاعدة قانونية جديدة تعمل على تنظيم استخدام هجمات الفضاء الإلكتروني في حالة الدفاع الشرعي عن النفس. فإذا ما استندت الدول إلى مثل ذلك في مواجهة هجمات الفضاء الإلكتروني بصورة فردية، فإنها تحمل تقديرًا لعدم مشروعية العمل المبرر للردِّ، وتتطلب أن يتمَّ تأكيد أن تلك التدابير تلعب دورًا أكثر فاعلية في العلاقات الدولية من أعمال الانتقام غير المبرَّر. وقد تنطوي تدابير الردِّ بالمثل

على تعسُّف في استعمال الحق، أو تمثل شكلاً من أشكال التدخل في الشئون الداخلية للدولة الذي حرصت على حمايته مواثيق الأمم المتحدة والحفاظ عليه.

تحمل هذه التدابير ردًّا على عمل غير مشروع دوليًّا، ومن ثم فإنها تلعب دورًا مهمًّا في إنفاذ القانون الدولي شأنها في ذلك شأن تدابير الانتقام. كما قد تُعَدُّ نوعًا من الجزاءات بالمعنى الفني الدقيق. وقد تكون تلك التدابير مؤقتة أو تنفيذية أو إكراهية أو عقابية، بما يطرح مشكلة وضع نصوص تعمل على أن تقوم دولة بعمل إجراءات لحماية دولة أخرى في حالة التعرُّض لمثل تلك الهجمات؛ حيث لا يوجد إطار قانوني يعاقب الدولة إذا ما امتنعت عن القيام بذلك.

هناك تحدٍّ آخر يتعلق بالحاجة إلى أن يتبنى المجتمع الدولي نظام قانون دولي يتعامل مع التنظيم الفعال لاستخدام هجمات الفضاء الإلكتروني وحرب المعلومات وأي أنشطة قد ترتبط بها والتمييز بينها، وتستطيع أن تتعامل مع أسلحة إلكترونية حديثة وتكتيكاتها، والتي قد تكون أدوات في أيدي فاعلين عدوانيين. وكذلك إيجاد مفهوم واضح للهجوم المسلح.

كذلك هناك تحدٍّ يتعلق بصعوبة التمييز بين هجمات شبكات الكمبيوتر التي ترتبط بالنشاط الإجرامي عن الأخرى التي ترتبط بأنماط الإرهاب وعن النشاط الذي تقف وراءه وتسانده الدولة.

كما أن هناك عددًا من المفاهيم والتعريفات التي ترتبط بالحرب في الفضاء الإلكتروني، ويمكن تفسيرها بطرق عديدة تبعًا لمن يستخدمها والهدف من ورائها، والذي يصعب تحديده بسهولة.

أما القضية الأخطر التي يمكن أن تثار في إطار محاولة تنظيم هجمات شبكات الكمبيوتر، والتي لم يتم تناولها في القواعد القانونية الخاصة بالدفاع الشرعي، فهي تتبدى في أبهى حللها في أن الفضاء الإلكتروني يحمل بعدًا عسكريًّا إلى جانب أنه يحمل في الوقت نفسه بعدًا مدنيًّا، وهذا ما يحتاج إلى تحديد مقتضيات وخصائص الهجوم الذي يُعَدُّ عدوانًا

وحربًا وإرهابًا ومبدأ الدفاع الشرعي عن النفس بصفة خاصة، وما يمكن أن يتعلق بالجهد الدفاعي أمام تلك الهجمات.

تتطلب عملية دفاع وهجوم حرب المعلومات وهجمات الفضاء الإلكتروني تعاونًا بنّاء ما بين كلٍّ من القطاع العام والقطاع الخاص والشركات العاملة في مجال المعلومات وتكنولوجيا الاتصال والمعلومات داخل الدولة؛ حيث يتميز مجال تكنولوجيا الاتصال والمعلومات بأنه من المجالات القليلة التي تحمل استخدامًا مزدوجًا ما بين المدني والعسكري.

هناك تحدٍّ خطير يتعلق بإمكانية المواءمة ما بين الهجوم والردِّ عليه، وشرط التناسب مع فعل الاعتداء الذي هو شرط من شروط الدفاع الشرعي عن النفس وفق القانون الدولي؛ حيث إن شبكات الكمبيوتر تسمح بتعدي آثار الاعتداء لأكثر من دولة. كما أن الردَّ على مثل هذا الاعتداء يتعدى أيضًا أكثر من دولة، دون القدرة على تحديد مصدر الهجمات. ومن ثم فإن الدفاع الشرعي يصبح عدوانًا؛ وذلك لعدم قدرته على التمييز. بالإضافة إلى إمكانية إحداثه أضرارًا لا مبرر لها؛ حيت يمكن أن تطول مرافق حيوية، والتي فرض القانون الدولي حماية خاصة لها في أثناء النزاعات المسلحة.

لا يوجد في مبدأ حظر استخدام القوة في العلاقات الدولية أي إلزام قانوني للدول داخل المجتمع الدولي بالوقوف جنبًا إلى جنب مع المعتدَى عليه لمواجهة العدوان. ومن ثم فإن القواعد القانونية التي تنظم استخدام القوة في حالة الدفاع الشرعي عن النفس ضد الهجمات لا توفر ضمانة للالتزام بها. كما لا توجد قواعد واضحة تحدد أن هناك دولة في حالة هجوم إلكتروني، وذلك قياسًا للطبيعة الإلكترونية والتكنولوجية التي يحدث بها فعل الاعتداء؛ حيث لا يستطيع مَن تعرَّض للهجوم أن يحدد تعرُّضه إلا بعد وقوع آثار فعلية تنتج عن هذا الاعتداء، نظرًا لأن التعرُّض يكون فجائيًّا، وهذا ما يكون له تأثيرات واضحة على الأمن والسلم الدوليين.

قد أثارت محاولة تطبيق مبدأ الدفاع الشرعي على هجمات الفضاء الإلكتروني رؤًى مختلفة حول مدى المواءمة القانونية وتطبيقاتها على تلك الهجمات، لا سيما وأن ميثاق الأمم المتحدة لم يتناول على وجه التحديد مفهوم الضربات الوقائية للدفاع عن النفس. فوفقًا إلى التفسير المتشدد فإن حق الدفاع الشرعي عن النفس يتمُّ فقط من جانب الدول للردِّ على هجوم مسلح. وهناك من يرى من الفقهاء أن ميثاق الأمم المتحدة لم يذكر ذلك صراحة؛ لاعتبار أن حق الدفاع الوقائي عن النفس يدخل ضمن العرف الدولي. ولكن يمكن استخدام السلاح الإلكتروني باعتباره واحدًا من أدوات النزاع المسلح في حالة الدفاع الشرعي عن النفس، فيمكن أن يُعَدَّ استخدام هذا السلاح لصدِّ عدوان مسلح يقوم على استخدام السلاح ذاته.

ويصبح استخدام الفضاء الإلكتروني كأداة من أدوات النزاع المسلح – ولو كان في إطار الدفاع ولمواجهة عدوان مسلح بهذا النوع من الأسلحة – عملاً غير مشروع؛ لأنه إذا كانت الدولة المعتدَى عليها تملك قانونًا حقَّ استخدام كل ما لديها من أسلحة وإمكانات عسكرية لدرء العدوان الواقع عليها، فإن هذا الاستخدام لكي يكون مشروعًا يجب أن يكون متفقًا والمبادئ الأساسية للقانون الدولي الإنساني، باعتبارها مبادئ عرفية واجبة التطبيق في جميع الظروف والأحوال، ومتماشية مع مبادئ قانون الحرب ومشروعية هجمات الفضاء الإلكتروني.

في السابق تمت إثارة الجدل حول مدى اعتبار استخدام الأسلحة الكيماوية أو البيولوجية تعبيرًا عن استخدام القوة المسلحة، وذلك على الرغم من أنها بمثابة وسيلة يمكن أن تتسبب في وقوع جرحى وقتلى مقارنة بالأسلحة التقليدية عن طريق استخدام الفيروس الحيوي أو الكيماوي. وعلى السياق نفسه، فإن هجمات شبكة الكمبيوتر والإرهاب الإلكتروني يتمُّ فيها توظيف الإلكترون لكي يتسبب في التدمير أو سقوط المصابين والجرحى، دون أن يتم توصيف تلك الهجمات على أنها تُعَدُّ «هجومًا مسلحًا».

تكون هجمات الفضاء الإلكتروني جزءًا من عملية عسكرية شاملة في حالة النزاع المسلح، وإذا كانت تمثل هجومًا وشيكًا ويمكن أن تتسبب في أضرار لا يمكن تجنُّبها.



ويمكن اعتبار هجمات الفضاء الإلكتروني جزءًا من النزاع المسلح، إذا كانت مواكبة له أو تكون منفصلة عنه دون أن تكون هناك حالة عدائية ظاهرة. ويفرض ذلك إشكاليات التعامل مع المسئولية القانونية عن تلك الهجمات. وتتوقف مسألة خضوع هجمات الفضاء الإلكتروني للقانون الدولي على وجود عدد من المتطلبات، منها: أنه يمكن اعتبارها استخدامًا للقوة، إذا ما هدف ذلك الهجوم الدولي لإحداث الضرر المباشر بأهداف مدنية، أو تسبب في جرحى، أو هدد الوجود الإنساني. أمَّا في حالة عدم اعتبار هجمات الفضاء الإلكتروني جزءًا من استخدام القوة ولكي يتم تطبيق ميثاق الأمم المتحدة عليها، فإن طبيعة الهجوم وخصائصه وآثاره تدلُّ على أنه استخدام للقوة.

إذا ما كانت هجمات الكمبيوتر والإرهاب الإلكتروني تتمُّ تعبيرًا عن استخدام للقوة غير المسلحة أو غيرها، فإنها تخضع للفصل السابع من ميثاق الأمم المتحدة ومبدأ الدفاع الشرعي عن النفس، ومن ثم يمكن أن يتمَّ الحكم بمدى مشروعية ذلك الهجوم إذا تمَّ استخدام القوة بشكلها المسلح في الهجوم. ويمكن أن تخضع هجمات الفضاء الإلكتروني لنصِّ المادة ٢-٤ وكذلك القانون الدولي العرفي والتي منعت جميعها استخدام القوة في العلاقات الدولية. وفي حالة استخدام القوة ليس فقط بشكلها المسلح ولكن تنطوي على ما من شأنه أن يحمل أي أعمال عدائية، وإذا لم ترقَ هجمات الفضاء الإلكتروني لمستوى استخدام القوة، فإنه يمكن النظر إليها باعتبارها تدخلاً في الشئون الداخلية للدول الأخرى، وهو ما يحرمه الميثاق.

في حالة استخدام تلك القوة من قِبل الدول عن طريق الهجوم باستخدام شبكات الكمبيوتر، وأمكن لمجلس الأمن أن يصف ذلك على أنه عمل من أعمال العدوان أو يمثل تهديدًا للسلم الدولي، ففي هذه الحالة يمكن إخضاعه لنص المادة ٢-٤ من الميثاق. وفي حالة إذا لم تأتِ هجمات شبكات الكمبيوتر في شكل هجوم مسلح، فإن مجلس الأمن قد يرى فيها تهديدًا للسلم الدولي، وبما يخوله من حق استخدام القوة لمنع تهديد السلم الدولي. والدول سواء أكانت بشكل فردي أم مجموعات قد تستخدم هجمات الفضاء الإلكتروني بشكلها المسلح للدفاع الشرعي وفق المادة ٥١ من الميثاق. كما أن الدول قد تستجيب



بشكل فردي أو جماعي إلى التهديد باستخدام تلك الهجمات غير مسلحة الطابع بردٍّ فعل ليس عسكريًّا بالضرورة.

قد يأتي ردُّ الفعل الشرعي في شكل إجراءات حماية أو تعاون أمني مشترك، ومن ثم فإن مسألة الدفاع الشرعي قد تتضمن جزأين: الأول يتم من خلال: دعم البنية التحتية للمعلومات، تأمين الفضاء الإلكتروني، دعم التعاون الدولي. أما الثاني فهو يأتي بعد التعرُّض للهجمات أو في أثنائها... أي أن الدفاع قد يكون عبارة عن ردِّ فعل أو له طابع وقائي. ويمكن أن تُعَدَّ مسألة استخدام أسلحة الفضاء الإلكتروني بكل أنواعها مخالفة – في حالة استخدامها – لمبدأ التناسب، وهو أحد المبادئ الجوهرية التي تكون واجبة التطبيق في حالة النزاعات المسلحة بكل أنواعها الدولية والداخلية. ويرمي هذا المبدأ إلى الإقلال من الخسائر أو أوجه المعاناة المترتبة على العمليات العسكرية، سواء بالنسبة للأشخاص أو الأشياء. ومن ثم فإذا كانت وسائل القتال المستخدمة لا يوجد تناسب بينها وبين الميزة العسكرية المرجوة من العملية العسكرية، فلا يجوز استخدامها[١٢٥].

يُعَدُّ شنُّ هجمات ضد البنية التحتية الكونية للمعلومات امتدادًا تلقائيًّا لاستخدام القوة في العلاقات الدولية. ووفق هذا التحليل فإن الدول قد تلجأ للردِّ على هذا الهجوم ليس فقط في إطار الردِّ التناسبي للدفاع الشرعي، ولكن أيضًا قد يأخذ شكل الضربات الوقائية للدفاع الشرعي، حتى في حالة ما لم يتم اعتبار هجمات الفضاء الإلكتروني ضمن تعريف ميثاق الأمم المتحدة للهجوم المسلح في المادة ٥١. ويعني ذلك اتساع استخدام حق الدفاع الشرعي، بما يدخل ضمن الأعمال العدائية التي يجرمها القانون الدولي؛ حيث يقرُّ القانون الدولي بعدة ضوابط لاستخدام حق الدفاع الشرعي، والذي يستلزم الوقوع تحت خطر «الهجوم الوشيك».

(١٢٥) كما ورد في المادتين: «المـادة ٥١: حماية السكان المدنيين»، تحت «الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف، ١٩٧٧»، **اللجنة الدولية للصليب الأحمر**، https://www.icrc.org/ara/resources/documents/misc/5ntccf.htm؛ «المـادة ٥٧: الاحتياطات أثناء الهجوم»، تحت «الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف، ١٩٧٧»، **اللجنة الدولية للصليب الأحمر**، https://www.icrc.org/ara/resources/documents/misc/5ntccf.htm.

سيؤدي ذلك إلى اتساع استخدام القوة تحت ذريعة الدفاع الشرعي. كما أن الأخطار غير العسكرية يمكن أن ترتفع بدرجة التهديد لمستوى الهجوم المسلح الذي «يصبح له تداعيات دولية من خلال انتهاك السيادة الإقليمية لدولة أخرى». إن أخطار الأعمال غير ذات الطابع العسكري التي يمكن استخدامها من قِبل الدول من الممكن أن تُعَدُّ هجومًا مسلحًا أو تصل إلى مستواه، وذلك عندما تتسبب في هجوم ذي طابع دولي يؤدي إلى أثر تدميري في دولة أخرى ذات سيادة. وأصبحت تتطلب تلك الصراعات غير التقليدية استجابات غير تقليدية.

يمكن أن تأتي عملية الهجوم من خلال الفضاء الإلكتروني باعتبارها جزءًا من حرب مستقلة أو جزءًا متواكبًا مع الحرب التقليدية، أو أن تقوم بها جماعات إرهابية ضد دول معينة، أو يقوم بها قراصنة. والواضح أنه لم يتوصل المجتمع الدولي إلى تقنين واضح وصريح بشأن الموقف من استخدام حرب المعلومات والإرهاب الإلكتروني أو التهديد بها، سواء وقت السلم أو الحرب. وبناءً عليه فإن ما يمكن الارتكاز عليه هو تعارض تلك الحرب مع ما استقرَّ عليه العرف والقوانين الدولية، ومنها القانون الدولي الإنساني.

جدير بالذكر أن هناك جهودًا مضنية دارت حول فكرة التجريم الدولي لأسلحة الدمار الشامل وفق مبدأ حظر التهديد باستخدام القوة في العلاقات الدولية وفق ميثاق الأمم المتحدة.

يبرز دور المحكمة الجنائية الدولية ومحكمة العدل الدولية في تولي مهمة وضع تشريع دولي يحرِّم استخدام الحرب المعلوماتية ضد الأماكن الحيوية، أو يقنن استخدامها أو التهديد بها وفق قانون الحرب. واستقرَّ العمل الدولي على التزام المقاتل في الحرب بصفة عامة بعدم استعمال الأسلحة أو المواد المحرمة أثناء العمليات الحربية؛ نظرًا لما ينطوي عليه ذلك من تجاوز للحدود التي يرسمها قانون الحرب والذي يستمد مصادره من الاتفاقيات الدولية العديدة، والذي أقرَّ بأن حقَّ المتحاربين ليس مطلقًا في اختيار وسائل الإضرار ببعضهم(١٢٦). وأيضًا لما يمكن أن تسببه من أضرار للمدنيين، وعدم التمييز بين المقاتلين وغير المقاتلين،

---

(١٢٦) إبراهيم محمد العناني، «المحكمة الجنائية الدولية ومنع انتشار أسلحة الدمار الشامل»، الفصل الثالث في **الخيار النووي في الشرق الأوسط: أعمال الندوة الفكرية التي نظمها مركز دراسات المستقبل بجامعة أسيوط** (بيروت: مركز دراسات الوحدة العربية، ٢٠٠١): ١٠٣–١١٩.



وإمكانية إصابة منشآت حيوية تتعلق بالبنية التحتية الكونية، خاصة فيما يتعلق بعدم إمكانية التحكم في حجم الضرر وعلاقته بأمن المجتمع الدولي[١٢٧].

أقرَّ ميثاق الأمم المتحدة في الفقرة ٤ من المادة ٢ منه بأن «يمتنع أعضاء الهيئة جميعًا في علاقاتهم عن التهديد باستعمال القوة واستخدامها ضد سلامة أراضي أو الاستقلال السياسي لأي دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة». وتؤكد طبيعة الالتزام بتقييد استخدام القوة أنه ذو طابع سلبي؛ بحيث تمتنع الدول عن اللجوء إلى القوة، ويُعَدُّ نطاق الالتزام بعدم استخدام القوة التزامًا شاملاً.

كما أن استخدام هجمات الفضاء الإلكتروني قد يدخل ضمن أعمال الانتقام العسكرية التي لا تتفق مع روح الميثاق، ويتعارض صراحة مع الإعلان الصادر عن الجمعية العامة للأمم المتحدة بخصوص المبادئ التي تحكم العلاقات الودية بين الدول لعام ١٩٧٠، والذي ينصُّ صراحة على واجب الدول في الامتناع عن أعمال الانتقام العسكرية. ويُعَدُّ الفضاء الإلكتروني في ظل تلك المادة نوعًا من العدوان غير المباشر وما يمكن أن يرتب من مسئولية دولية عن تلك الأفعال، التي تعدها الدولة المعتدَى عليها عدوانًا من دولة أخرى، وبما قد يؤدي إلى احتدام حدة الصراع بشكله التقليدي وغير التقليدي، وبما يشبه حالة الفوضى التي تمتد آثارها إلى العالم أجمع الذي يرتبط بالبنية التحتية الكونية للمعلومات، ومع وجود فاعلين من غير الدول وعدم وضوح الجهة المعتدية.

تدفع عدم واقعية المبدأ الخاص بتناسب الردِّ في حالة الدفاع الشرعي مع استخدام هجمات الفضاء الإلكتروني إلى صعوبة القياس أو التحكم في تلك الهجمات، وكذلك عدم التحقُّق من مبدأ الملاءمة من الناحية القانونية. ويأتي هنا دور المادة ٤١ التي تقرر بأن «لمجلس الأمن أن يقرر ما يجب اتخاذه من التدابير التي لا تتطلب استخدام القوات المسلحة لتنفيذ قراراته، وله أن يطلب إلى أعضاء الأمم المتحدة تطبيق هذه التدابير، ويجوز أن يكون من بينها وقف الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبريدية

(١٢٧) أحمد عبد الونيس شتا، «القانون الدولي والأسلحة النووية»، في **أعمال ندوة «إخلاء منطقة الشرق الأوسط من أسلحة الدمار الشامل: الجوانب القانونية»** (القاهرة: جامعة القاهرة. كلية الاقتصاد والعلوم السياسية، ٢٠٠٤).

والبرقية واللاسلكية وغيرها من وسائل المواصلات وقفًا جزئيًّا أو كليًّا وقطع العلاقات الدبلوماسية»[١٢٨].

يمكن أن يتسبب استخدام هجمات الفضاء الإلكتروني في حالة الدفاع الشرعي في تدمير مباشر وغير مباشر أو إحداث ضرر بالمدنيين غير مبرَّر، بما يشكل صعوبة تنفيذ أو استخدام حقِّ الدفاع الشرعي عن النفس، وبما يتعارض مع نصِّ المادة ٥١ التي تقضي بأنه «ليس في هذا الميثاق ما يُضعف الحق الطبيعي للدول أو ينتقص منه، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلَّغ إلى المجلس فورًا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس – بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق – من حق في أن يتخذ في أي وقت ما يراه ضروريًّا لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه». ويمكن لهجمات شبكات الاتصال والمعلومات بواسطة شنِّ هجمات الفضاء الإلكتروني أن تنشر الدمار وتتسبب في وقوع خسائر اقتصادية وتُلحق أضرارًا بالحياة المدنية، والتي يمكن أن تدخل ضمن أعمال مجلس الأمن واختصاصه باعتباره هيئة دولية تختصُّ بالسلم والأمن الدوليين.

(١٢٨) «المادة ٤١»، تحت «الفصل السابع: فيما يتخذ من الأعمال في حالات تهديد السلم والإخلال به ووقوع العدوان»، في **ميثاق الأمم المتحدة**.

المبحث الخامس

التحديات والإشكاليات في سبيل التعاطي القانوني مع الأسلحة الإلكترونية

أولاً: إشكاليات تطبيق القانون الدولي على هجمات الأسلحة الإلكترونية

يتضمن القانون الدولي بالأساس احتمالات واقعية مادية سواء في مجرياتها أو نتائجها أو آثارها. كما أنه حتى لو تم تضمينه هجمات الفضاء الإلكتروني باعتبارها حالة نزاع مسلح(١٢٩)، فإنه يصعب تصنيفها على أنها حالة هجوم؛ حيث إن الهجوم على المدنيين أو المنشآت المدنية قد لا يسفر عن وقوع ضحايا أو جرحى، وذلك خلاف ما يحدث في الهجوم التقليدي؛ حيث يحظى المدنيون بحماية القانون الدولي. ومن ثم فإن هجمات الفضاء الإلكتروني قد لا تُعَدُّ هجومًا بالمعنى التقليدي، وكذلك دورها في فتح المجال لاحتمال إصابة أشخاص أو أهداف تحظى بالحماية وغير متوقعة ولا يحميها القانون الدولي.

من ثَمَّ فإن الجهود الدولية لإقرار الحماية من التعرُّض لهجمات الفضاء الإلكتروني لا ترقى إلى مستوى العمليات الوقائية، وهي لا تزيد على كونها عمليات إغاثية، وبما يجعل هناك تشجيعًا أكبر على تنفيذ الأهداف العسكرية بسهولة مع تقليل حجم الخسائر أو الإصابات العرضية عبر الفضاء الإلكتروني بخلاف الهجوم العادي التقليدي. ومن ثم فإن ذلك سيمثل إغراءً لاستخدامها من قادة الحرب، وتظهر مسألة الخلط الواضح بين مفهومي الفضاء والحرب. ومن هنا يتم النظر في مدى مشروعية العدوان والحرب، وقدرة القانون الدولي على أن يميِّز بينهما لكي يتم تطبيق قواعد وأحكام معينة خاصة بها.

يواجه هذا الهجوم تحديات تتعلق بطبيعة الفهم التقليدي لحالة المقاومة؛ لأن استخدام المدنيين للتكنولوجيا ومعرفة كيفية الاتصال بالعمليات العسكرية عن طريق الفضاء الإلكتروني من الممكن أن يساعد في انحسار آثار العدوان، أو مدى ما يجب أن يتوافر لهؤلاء المدنيين من حماية تحت حالة الحرب، وأن طبيعة شبكات الاتصال والمعلومات الدولية تفرض قيودًا على الدول من أجل الخضوع إلى معايير أمان أو حماية، وبما قد يتعارض مع سيادتها وحقِّها

(١٢٩) نبيل أحمد حلمي، **القانون الدولي وفقًا لقواعد القانون الدولي العام**، (القاهرة: دار النهضة العربية، ١٩٩٩): ١٢٠-٢٠٠.



في إدارة شئونها الداخلية بدون تدخل خارجي كما قضت بذلك محكمة العدل الدولية بشأن نيكاراجوا[١٣٠].

هناك حالة الجرف القاري لبحر الشمال التي أكدت فيها محكمة العدل الدولية أهمية العرف باعتباره مصدرًا من مصادر القانون الدولي[١٣١]. فمنذ اتفاق ويستفاليا عام ١٦٤٨، الذي أكد سيادة الدولة المطلقة على كامل أراضيها داخل حدودها المعترف بها دوليًّا، أصبح مفهوم السيادة غير ملائم للتطبيق مع درجة التشبيك العالية بين دول العالم، ووجود فضاء إلكتروني وعالم شبكي عابر للحدود الدولية والسيادة الإقليمية للدول. وأوجدت هجمات الفضاء الإلكتروني صعوبة في تحديد مفاهيم السلام والحرب وتحديد الأهداف وطبيعتها المدنية والعسكرية. ويصبح الضرر غير الملموس للإرهاب الإلكتروني باعتباره هجومًا لا يمكن أن ينطبق عليه القانون الدولي الإنساني أو قانون الحرب الذي هدف إلى حماية المدنيين. وهناك إشكالية حول تحديد المسئولية القانونية خلف الهجمات، وخاصة أن الدول التي قد تعاني هجمات الفضاء الإلكتروني قد تصاحبها حالة من التوترات الدولية العالية.

من ثَمَّ تكون هناك صعوبة في تمييز ذلك الهجوم والتحقق بشأنه. كما أنه حتى إذا أخذت الهجمات مجرد رد فعل، فإنها قد لا تستطيع التمييز بين الأطراف، ومن ثم فإنها تصبح غير قانونية وذلك لعبور الشبكات الحدود الدولية وإصابة أطراف محايدة. وإن التحقيقات بشأن هجمات الفضاء الإلكتروني قد تجمع بين المبادئ الأساسية لعمل أجهزة الاستخبارات بوصفها عملاً طبيعيًّا ماديًّا وبين الإلكتروني العابر للشبكات والحدود الدولية. لكن عملاء أجهزة الاستخبارات الدولية قد لا يستطيعون الولوج إلى دول أخرى؛ لأنها ستعد ذلك انتهاكًا لسيادتها.

(١٣٠) عندما تدخلت الولايات المتحدة في نيكاراجوا عام ١٩٨٦ كان رأي محكمة العدل الدولية يختلف عن الرأي الأمريكي الذي كان يرتكز على «أن نيكاراجوا اختارت نظامًا شموليًّا ديكتاتوريًّا شيوعيًّا» فقضت المحكمة بأنه «ليس لأي طرف الحق في التدخل في اختيار شعب لنظامه السياسي» وعندما ردت الولايات المتحدة الأمريكية تقول: «إن نيكاراجوا تمتلك أسلحة تهدد بها الأمن في المنطقة» ردت محكمة العدل الدولية بأنه «لا يوجد في القانون الدولي ما يُحدُّ دولة من تملكها لأسلحة ما في غير نطاق المعاهدات الدولية».

(١٣١) "North Sea Continental Shelf (Federal Republic of Germany/Netherlands): Proceedings Joined with North Sea Continental Shelf (Federal Republic of Germany/Denmark) on 26 April 1968". International Court of Justice, http://www.icj-cij.org/docket/index.php?sum=295&code=cs2&p1=3&p2=3&case=52&k=cc&p3=5.



قد يأتي الهجوم الإلكتروني من أكثر من دولة أو من فاعلين من غير الدول، وتتطلب مواجهته الحاجة لتعاون دولي، ودعم المساعدة في الحماية ضد الأخطار المشتركة، أو حتى حمل الحكومات المحلية على تقديمها بشأن هجمات كان مصدرها أراضيها، مع عدم وجود اتفاق عالمي حول التعريف القانوني للسلوك الإرهابي، خاصة أن المجتمع الدولي إلى الآن لم يصل إلى تعريف واضح للإرهاب بشكله التقليدي، ناهيك عن الفضاء عبر الإنترنت. فهناك من الدول من يعتبر الإرهاب سلوكًا جنائيًّا وجريمة، والبعض الآخر يعتبر الإرهاب مقاومة مشروعة أو جريمة سياسية.

هناك تداخل لمفهوم الإرهاب الإلكتروني مع غيره من المفاهيم كـ: الجريمة الإلكترونية والمنظمة، الاحتيال، التجسس، قرصنة المعلومات، حرب المعلومات، غيرها. وقد فرض ذلك إشكالية تحديد المعاملة القانونية الواضحة. ويمثل عنصر المباغتة الذي يتميز به الفضاء الإلكتروني – خاصة في بعده الرقمي – تحديًا أمنيًّا يضع الطرف الأخير في موقف ضعيف؛ حيث يقتصر دوره في تلك الحالة على ردِّ الفعل، مع إصابة الإجراءات الوقائية في مقتل. وتطرح مسألة تعدُّد الفاعلين قضية المسئولية القانونية، وخاصة أن استخدامه قد لا يقتصر على الجماعات والأفراد، بل قد تستخدمه الدول أيضًا.

ويضفي البعد الدولي للظاهرة تعقيدًا في شأن المواجهة الدولية، خاصة مع عدم وجود إطار قانوني دولي واضح لتناول تلك الظاهرة المستحدثة. وقد يستلزم ذلك: إما الحاجة لقانون دولي جديد، أو عقد اتفاقيات مكملة للاتفاقيات الدولية، أو تفعيل اتفاقيات أخرى قائمة.

وقد اعتمدت بلدان عديدة تشريعات لمكافحة الاستخدام غير السلمي للفضاء الإلكتروني، أو في سبيلها لاتخاذ مثل تلك التشريعات. ويتم اتخاذ مثل تلك التشريعات لكي يتم تنفيذها داخل الحدود الجغرافية للدولة. ولكن تبقى هناك صعوبة في حالة إذا ما تم ارتكاب جريمة في مكانٍ أو دولةٍ ما وتم التحريض في دولة أخرى، وذلك ما لم تكن هذه الأطر القانونية قابلة للتطبيقٍ على نحوٍ تبادلي بين البلدان.

ولكي يتم تطبيق القانون الدولي على هجمات الفضاء الإلكتروني يجب أن يتم:

أولاً: قبول التفسيرات المتعددة التي قامت على أساس تفسير «الصراع المسلح» ومفهوم «الهجوم» بما يتناسب مع التطور في آليات الهجوم وأدواته ويتفق مع روح القانون الدولي؛ حيث إن غياب ذلك يجعل من الصعوبة بمكان تطبيق القانون الدولي الإنساني على هجمات الفضاء الإلكتروني.

ثانيًا: إن هجمات الفضاء الإلكتروني يمكن اعتبارها هجومًا من منطلق إمكانية استهدافها العديد من المنشآت المحمية أو الأشخاص، وهذا من شأنه أن يؤدي إلى اتساع ما يمكن أن يُطلق عليه «أهداف الحرب».

ثالثًا: بالنظر إلى حقيقة أن هجمات الفضاء الإلكتروني يمكن أن تمثل وسيلة حربية بدون إحداث أضرار أو جرحى بالمقارنة بالهجمات التقليدية.

رابعًا: إن هجمات شبكات الكمبيوتر والإرهاب الإلكتروني تضع تحديات تتعلق بمدلولات «الهجوم»، كما أنها ستختبر الفهم التقليدي لحالة المحارب وذلك بسبب الاستخدام المدني للتكنولوجيا، ومعرفة كيفية اتصالها بالعمل العسكري عن طريق الكمبيوتر. وهناك فشل في وضع حدود معينة حول مشاركة المدنيين في الأعمال العدائية، وهذا ما يُضعف القانون الدولي الإنساني.

وضع مايكل شميت عددًا من المؤشرات لتحديد متى يمكن اعتبار هجمات الفضاء الإلكتروني استخدامًا للقوة، وذلك من خلال درجات تتراوح ما بين (١–١٠). وفي حالة تطبيق تلك المؤشرات والوصول إلى درجة ٧ فإنها تُعَدُّ استخدامًا للقوة. وهذه المؤشرات هي: قسوة الهجوم Severity إذا ما كان المدنيون معرضين للقتل أو الضرر الجسيم بالممتلكات، فإن ذلك العمل يعد عملاً عسكريًا. وحتى إذا كان الضرر أقل أو مشابهًا فإنه يُعَدُّ استخدامًا للقوة. وتوافر الآنية Immediacy؛ حيث تتم رؤية آثار الهجوم من خلال رؤيتها في دقائق أو ثوانٍ، كما يحدث عند انفجار قنبلة تقليدية[١٣٢].

(١٣٢) Schmitt, *Computer Networks Attack*.

وإذا أخذ العمل العسكري مدة تصل إلى أسابيع أو شهور، فإنها تصبح عملاً دبلوماسيًّا أو اقتصاديًّا. وأيضًا أن يكون العمل العسكري مباشرًا Directness؛ حيث يكون الحدث نتيجة لسبب مباشر؛ حيث تكون هناك علاقة مباشرة بين السبب والنتيجة. وكذلك أن يخضع ذلك الفعل إلى القياس والملاحظة Measurability، حيث يمكن ملاحظة الحدث وقياسه كميًّا كحجم الخسائر المادية التي تنجم عن هذا الاستخدام. وأن يتوافر في ذلك العمل الاختراق Invasiveness؛ حيث يتم انتهاك الحدود الدولية والدخول غير الشرعي إلى المنشآت أو المؤسسات المحمية. وأن يتم افتراض شرعية العمل Presumptive؛ حيث يكون للدول الحقُّ في احتكار الاستخدام الشرعي للقوة. والمسئولية Responsibility؛ حيث يترتب على مسئولية الدولة عن العمل العسكري التزامات قانونية.

ثانيًا: محددات إعلان الفضاء الإلكتروني نظامًا خاليًا من انتشار الأسلحة الإلكترونية(١٣٣)

تختلف آليات التعامل مع الأسلحة الإلكترونية عن غيرها من الأسلحة غير التقليدية مثل الأسلحة النووية أو الكيماوية أو البيولوجية، وبخاصة أنها عجزت عن إقرار أحكام ملزمة للدول بالامتناع عن امتلاك تلك الأسلحة خارج إطار المعاهدات، وأنها لم تمنع إمكانيات التعاون بين الدول المالكة للسلاح النووي في تطويره أو إنتاجه، وركزت تلك الجهود الدولية على تعزيز احتكار الدول المالكة للسلاح النووي، وذلك على الرغم من أن القدرة على الإشراف والرقابة على تطوير الأسلحة غير التقليدية ممكنة مقارنة بالأسلحة الإلكترونية، والتي يتم استخدامها ضد البنية التحتية الكونية للمعلومات وهو ما يعرضها للخطر والدمار والتعطيل، بما يكون له من أثر على الدولة التي تكون ضحية لذلك الاعتداء، وأيضًا ما يتصل بتهديد المجتمع الدولي ككل عن طريق شبكات الاتصال والمعلومات التي تربط دول العالم بعضها ببعض وتزايد درجات الاعتماد المتبادل بين دول العالم، وما ينتج عن ذلك من انتهاك لقيم ومبادئ القانون الدولي الذي عمل على إرساء الاستخدام السلمي والتعاون والتفاهم بين شعوب العالم(١٣٤).

(١٣٣) عبد الصادق، **الفضاء الإلكتروني والعلاقات الدولية**: ٢٥٥-٢٦٥.

(١٣٤) عبد الصادق، **الإرهاب الإلكتروني: القوة في العلاقات الدولية**: ٢٣١-٢٣٤.

وتزايد عدد الدول التي تعمل على تطوير الأسلحة الإلكترونية وتصاعد حجم ونطاق استخدامها في الصراع الدولي، وفي ظل عدم وجود أي إطار قانوني يحمل على الحد من التسلح الإلكتروني، بالإضافة إلى المزايا الاستراتيجية لاستخدام وتطوير تلك الأسلحة وتصاعد احتمالات استخدام تلك الأسلحة من جانب الجماعات الإرهابية والإجرامية، وتأثير ذلك على الاستخدام المدني للفضاء الإلكتروني. وبخاصة مع حالة التداخل الشديد بين المدني والعسكري.

ويمكن أن ينمو سوق لتجارة الأسلحة الإلكترونية تنافس قدرات الدول، والتي يتم فيها توظيف المجرمين أو القراصنة أو المتطوعين بما يعمل على سرعة انتشارها ويفاقم من تأثيرها ويحد من قدرة الدول على تنظيم استخدام القوة عبر الفضاء الإلكتروني. وهو ما يمثل مزيدًا من تعقيدات إمكانية التحكم والسيطرة على منع مصادر التهديد الجديدة للفضاء الإلكتروني، وتعزيز قدرات الفاعلين من غير الدول الوصول إلى المواد اللازمة لإنتاج الأسلحة الإلكترونية، وهو ما يزيد من معاناة العالم من مخاطر امتلاك واستخدام الأسلحة الإلكترونية وتحمل تأثيرات هامة على الأمن العالمي.

وتتميز الأسلحة الإلكترونية بالتنوع في شكلها وقدراتها، ويأتي ذلك مع مخاطر انتشار التسلح الإلكتروني ووجود عدد من الدول تملك مقدرات تلك الأسلحة وأخرى تطورها، ودول تحاول الدخول إلى نادي هذا السلاح الإلكتروني الجديد إلى جانب إمكانية استخدامها من جانب الحركات الإرهابية أو الإجرامية. وتصاعدت حالات استخدام الأسلحة الإلكترونية، في الصراع الدولي والتوترات الدولية بين كافة الفرقاء في مجتمع المعلومات العالمي.

وتنامت لدى قطاعات واسعة من الرأي العام العالمي بالمخاطر التدميرية للأسلحة الإلكترونية والتي تضاهي في تأثيراتها عملية استخدام الأسلحة النووية وتأثيرها على أمن

الأفراد والدول والمجتمعات والمنشآت المدنية، إلا أنها تحولت إلى ساحة للصراع حول تطويرها بين الدول، وبدأت تتحول من الهجمات العشوائية إلى الطابع المنظم والأكثر دقة وتدميرًا والأكثر ذكاء في تنفيذ أهداف السياسة الخارجية للدول التي تستخدمها، وباتت الدول تخصص نفقات عسكرية لتطويرها، وتم تشكيل وحدات متخصصة داخل الجيوش في الحرب الإلكترونية عبر الفضاء الإلكتروني. والتي يعرفها ريشتارد كلارك بأنها «الإجراءات التي تتخذها دولة قومية لاختراق أجهزة الكمبيوتر الخاصة بدولة أخرى أو بإصابة الشبكات الخاصة بها لإلحاق أضرار أو تعطيل».

وتستهدف تلك الأسلحة إصابة نظم التحكم الصناعية، التي تثير قلقًا خاصًّا هي تلك المكونات التي تشرف على تشغيل محطات لإنتاج الطاقة وتقديم الخدمات مثل: مرافق المياه، وشبكات إمدادات الطاقة الكهربائية، ونظم السيطرة الأرضية والمستشفيات والمنشآت الحكومية، وشبكات الاتصالات، وأنظمة الدفاع، والملاحة الجوية وأنظمة السيطرة على المجال الجوي. والنظم المالية والأنظمة المصرفية، وتحول الفضاء الإلكتروني إلى ساحة لأسلحة انتشار شامل فيما يتعلق بحجم تأثيرها وانتشارها، وهو ما يجعلها تتميز عن غيرها من الأسلحة غير التقليدية والتي ترتبط بمحيط إقليمي محدد، وتتميز عملية استخدامها بأنها متعدية الحدود ولسيادة الدول وتميزها بسهولة تطويرها ونشرها واستخدامها ورخص تكلفتها مقارنة بالأسلحة التقليدية الأخرى بما يجعلها عنصر جذب هام لاستخدامها من قبل الدول في التوترات والحروب والصراع الدولي. وكذلك خطورة استخدامها من قبل جماعات إجرامية أو إرهابية في صراعها مع الدول أو مع غيرها بما ينعكس على أمن المجتمع الدولي وأمن الفضاء الإلكتروني والحضارة الإنسانية الحديثة [١٣٥].

محددات تعترض استخدام الأسلحة الإلكتروني كتعبير عن القوة في الفضاء الإلكتروني، ولعل أهمها:

١– عدم وضوح حجم تأثير عملية شن الهجوم عبر الفضاء الإلكتروني بسبب نقص المعرفة والخبرة النابعتين من التاريخ القصير لحرب الفضاء الإلكتروني. ويكون لعمليات هجوم معيّنة

(١٣٥) Paganini, "The Rise of Cyber Weapons and Relative Impact on Cyberspace".

مؤثرات محدودة بينما يكون لعمليات أخرى تأثيرات واسعة النطاق، ويمكن إلحاق ضرر غير مرغوب بأجهزة مدنية أو انتشار الهجمات في دول أخرى إلى جانب الدول المستهدفة.

٢- إنه من الصعوبة ترجمة هجوم الفضاء الإلكتروني إلى إنجاز سياسي. وفي حالة هجوم إلكتروني كهذا لا يوجد احتلال لأراضٍ أو لأهداف كي يتم استخدامها قاعدة لمفاوضات سياسية في مجال الحرب، مثلما يتم فعلًه في الحرب البرية.

٣- هناك صعوبة في ضمان استمراريّة عملية شن الهجوم المتواصل في مجال الفضاء الإلكتروني. وفي كثير من الحالات بمقدور الخصم أو الطرف المستهدف أن يعمل على سد ثغرات الاختراق واستعادة أنظمته بسرعة عالية نسبيًّا لإصلاح أضرار الهجوم الإلكتروني. وهو ما يؤثر على إمكانية تراكم الأضرار ومن ثم إحداث ضغط سياسي كما هو الحال في سلسلة هجمات جوية استراتيجية. وهو ما يمثل خللاً في قوة الذراع الهجومي للفضاء الإلكتروني.

٤- هناك مخاطر من ردة فعل مضادة في حالة التعرض للهجوم عبر الفضاء الإلكتروني والذي من شأنه أن يُعرّض الدولة المهاجمة لضربة مضادة، ويُحتمل أن يأتي الرد من خارج مجال الفضاء الإلكتروني. وتصبح قوة الردع مختلفة ولدى الولايات المتحدة قوة كبيرة تفوق ما يوفره الفضاء الإلكتروني للمُهاجِم لحمايته من شن هجوم مضاد وهو غير متوفر لمعظم الدول الأخرى.

٥- تكون المخاطر التي تتعرض لها الدولة المُهاجِمة بالغة طالما أنها تعتمد كثيرًا على مجال الفضاء الإلكتروني في استخداماتها، «بيت من الزجاج». وطالما أن منظومة دفاعها ضعيفة جدًّا. وترتبط الدول الرائدة في قدرات الهجوم في الفضاء الإلكتروني بدرجات عالية من الارتباط به، ومن ثم تكون حماية تلك الدول غير كافية، وعليه فهي تعرض نفسها لضرر بالغ. وهو ما قد يكبح سباق التسلح في الفضاء الإلكتروني.

٦- أن عملية استخدام الهجمات الإلكترونية في الصراع الدولي تحمل خطورة الإضرار بأطراف ثالثة ليس لها علاقة بموضوع الصراع، ولكن اشتراكها في استخدام الفضاء

الإلكتروني يؤهلها للتعرض للهجمات مثل دولة محايدة، أو شركة اتصالات دولية، وهو ما يؤدي إلى احتمال تصاعد ردود الأفعال من جانب الطرف الثالث أو من المنظومة الدولية باعتبار الفضاء الإلكتروني مرفقًا دوليًا.

٧- يمكن أن تؤدي عملية استخدام الأسلحة الإلكترونية إلى مخاطر قيام تحالفات سيبرانية متعارضة وعلى سبيل المثال أدى قيام روسيا بشن هجمات إلكترونية على إستونيا عام ٢٠٠٧ إلى إثارة الوعي بالأمن الإلكتروني وبحاجة الناتو للدفاع عن الدول الأعضاء في المنظمة، ومن ثم فقد أدى الهجوم الروسي ضعيف الأثر إلى استنهاض تحالف سيبراني ضدها.

٨- تمثل عملية استخدام الهجمات الإلكترونية مخاطر أمام المجتمع الدولي لاتساع حجم التأثير وعدم وجود نظام دولي ينظم العمليات في مجال الفضاء الإلكتروني. ومع ذلك، يُحتمل وقوع هجمات تؤدي إلى خسائر في الأرواح أو ضرر في منشآت الدولة، وهو ما يعد عملاً عدوانيًا وفق القانون الدولي. وهذا الوضع من شأنه استمرار حالة الفوضى وإلى سعي الدول دون هوادة في تطوير قدراتها في مجال التسليح الإلكتروني.

٩- يمكن أن تكشف قدرات الهجوم في الفضاء الإلكتروني للدولة المهاجمة عن قدراتها الاستراتيجية أمام جميع الأطراف الدولية، وهو ما يعمل على تعزيز وتسريع عملية التحصين والحماية والخبرة في مكافحة تلك الهجمات واحتوائها وقد يتم استخدام تلك الأدوات الجديدة (الفيروسات) بعد فهم آلية عملها في استخدام الدولة المستهدفة لها، وتتميز تلك الأسلحة أنها أحادية الاستخدام، فعندما يتم استخدامها لا يتم استخدامها مرة أخرى في هجمات لمعرفة طريقة عملها وكيفية احتوائها.

١٠- تتميز أهداف الهجمات بدرجة من التناقض بين أهدافها ما بين القيام بعملية لجمع المعلومات من الطرف المستهدف أو بالقيام بشن هجمات تخريبية لأنظمته المعلوماتية، إلى جانب صعوبة التمييز بين الأهداف المدنية والأخرى ذات الطابع العسكري.



١١– مثّل عدم وجود تعريف واضح لـ «الأسلحة الإلكترونية» نقطة ضعف هامة في الجهود الدولية لمكافحتها عملية انتشارها وتطويرها[١٣٦].

ثالثًا: محددات تطبيق نظريات الإخلاء والحد من التسلح في الفضاء الإلكتروني

تعززت الجهود الدولية في مجال مواجهة انتشار الأسلحة غير التقليدية كالنووية والكيماوية والبيولوجية وبخاصة مع تأثير عملية استخدامها على الجنس البشري، وتم تأسيس منظمات واتفاقيات للعمل على حظر استخدامها أو منع انتشارها، وعلى السياق ذاته فإنه بالقياس إلى تأثير استخدام الأسلحة الإلكترونية والتي يتم استخدامها على إلحاق أضرار للبنية التحتية الكونية للمعلومات وبمصالح مدنية وتضر بالاقتصاد العالمي، وبأمن الفضاء الإلكتروني وبخاصة مع قدرات الدول في تطوير أو إنتاج واستخدام الأسلحة الإلكترونية وبخاصة مع عدم وجود إطار قانوني أو تنظيمي للتعامل مع تلك الأسلحة، وعدم وجود اتفاقية دولية أو اتفاق دولي للحد من التسلح الإلكتروني أو منع أو تقييد استخدام الأسلحة الإلكترونية، وبخاصة مع المخاطر المتعلقة بإطلاق سباق تسلح غير قابل للسيطرة في الفضاء الإلكتروني، وكانت الجهود الدولية في التعامل مع أسلحة الدمار الشامل قد تكللت بعقد اتفاقيات للحد من التسلح وقيام وظهور «المنطقة الخالية في النظام الدولي» كما تم مع الأسلحة النووية في ديسمبر ١٩٧٥، وذلك عندما تقدمت المكسيك بطلب للجمعية العامة للأمم المتحدة لتعريف المناطق الخالية من الأسلحة النووية، وهو ما قامت به في قرارها رقم ٣٤٧٣ بتعريف المنطقة الخالية "Nuclear Weapon Free Zones "NWFZ.

وعلى الرغم من قوتها الدبلوماسية فإنها فشلت في وقف انتشار الأسلحة النووية ونجحت في إعلان بعض المناطق الإخلاء الطوعي من الأسلحة النووية، وعانت مبادرة إخلاء العالم من الأسلحة النووية من بعدها التمييزي بالعمل على احتفاظ النادي النووي بقدراته ومنع الآخرين من الدول في الدخول إليه، وكشف ذلك عن عدم استعداد الدول الكبرى التخلي عن أحد عناصر قوتها، وفي السياق ذاته إنه في حالة الأسلحة الإلكترونية عبر

(١٣٦) للمزيد حول تلك التطورات، انظر: **المركز العربي لأبحاث الفضاء الإلكتروني**، www.accronline.com.

الفضاء الإلكتروني ربما تكون مبادرة إخلائه منها شاملة وعامة لمجال الفضاء الإلكتروني لاعتبارات الاتساق والتواصل والوحدة الفيزيائية للفضاء الإلكتروني، ولكن تبقى الدعوة إلى إخلائه من التسلح الإلكتروني مرهونة بإرادة دولية ووعي عالمي بمخاطر استخدامها وبخاصة أن الفاعلين في استخدام تلك الأسلحة الجديدة قد لا يكونون بدول بل يمكن أن يكونوا من الجماعات الإرهابية أو الشركات التكنولوجية أو القراصنة أو المتطوعين.

ومن ثم فإن خطاب الإخلاء يجب أن يوجه إلى كافة الفاعلين في الفضاء الإلكتروني وبالأخص الدول المتقدمة تكنولوجيًا والشركات التكنولوجية الكبرى، وعلى أي حال فإن إقرار الفضاء الإلكتروني كمنطقة خالية من الأسلحة الإلكترونية Cyber Weapon Free Zone، يعد أحد أهم المبادرات الدبلوماسية بالإضافة إلى السعي إلى إقرار اتفاقية دولية للفضاء الإلكتروني تنظم الاستخدام وتوازن ما بين الحقوق والواجبات بين كافة الفاعلين في الفضاء الإلكتروني.

وتشمل عملية إخلاء الفضاء الإلكتروني من الأسلحة الإلكترونية وإقرار نظام دولي جديد يعمل على منع استخدامها أو انتشارها أو تطويرها أو بيعها أو العمل على إقرار اتفاق خاص يتعلق بتحديد نظام الخلو التام من الأسلحة الإلكترونية، والعمل على إنشاء جهاز دولي للتحقق والمراقبة لضمان الامتثال للالتزامات الناشئة، وتحديد الالتزامات الرئيسية للدول الحائزة على الأسلحة الإلكترونية تجاه الدول التي لا تمتلك القدرات الإلكترونية في الفضاء الإلكتروني. وإلى جانب السعي لتبني اتفاقية دولية للفضاء الإلكتروني وأخرى تتعلق بمنع التسلح داخل الفضاء الإلكتروني وربما يأتي ذلك في شكل معاهدة أو اتفاقية أو بروتوكول، أو ميثاق دولي، يعمل:

١- على أن يتم النص على احترام جميع عناصر نظام الخلو التام للفضاء الإلكتروني من الأسلحة الإلكترونية المحددة في المعاهدة أو الاتفاقية المنشئة لذلك.

٢- أن تمتنع عن الإسهام بأي طريقة في أداء أفعال من شأنها انتهاك للمعاهدة، أو للاتفاقية المذكورة آنفًا.



٣- أن تمتنع عن استعمال الأسلحة الإلكترونية أو التهديد باستعمالها ضد الدول الأخرى.

ومن الأهمية بمكان تحديد ماهية أن يصبح الفضاء الإلكتروني منطقة خالية من الأسلحة الإلكترونية والتي يمكن أن تتضمن عملية «تحويل الفضاء الإلكتروني كمجال جديد في العلاقات الدولية إلى منطقة خالية من الأسلحة الإلكترونية، والتي من شأن استخدامها أو التهديد بها أو تطويرها التأثير على الاستخدام السلمي للفضاء الإلكتروني وعلى نحو يضر بأهميته ودوره الاستراتيجي في خدمة المجتمع العالمي»، ومن ثم فإن عملية الإخلاء موجهة إلى كافة الفاعلين في مجتمع المعلومات العالمي على اعتبار أن الفضاء الإلكتروني مرفقًا دوليًا يشكل تهديده التأثير على أمن المجتمع العالمي قاطبة.

على الرغم من الصعوبة في عملية الرقابة والتفتيش على الأسلحة الإلكترونية فإن السعي نحو تفعيل عملية إقرار منطقة خالية يتطلب وجود نطاق دولي تتشارك فيه العديد من الدول والجماعات عبر العالم، إلى جانب وجود الإطار القانوني الدولي الذي يصبح بقدرته تحديد الالتزامات والواجبات والحقوق للفاعلين المشتركين في هذا النظام. والذين يصبح لهم نشاطات إلكترونية تنطوي على مخاطر لأمن الفضاء الإلكتروني، السعي لدى الدول على وضع قيود على صناعة وتطوير وتخزين وإطلاق أو اختبار وامتلاك الأسلحة الإلكترونية داخل نطاق الفضاء الإلكتروني، مع السماح للتعامل مع التطبيقات السلمية الأخرى في البرمجيات أو المعدات المرتبطة بالفضاء الإلكتروني. والتي قد تقع في المنطقة الفاصلة بين الاستخدام العسكري أو شبه العسكري وما بين الاستخدام المدني وهو ما يختلف عن طريقة التعامل مع: الالتزامات الأساسية في المناطق الخالية من الأسلحة النووية[١٣٧].

فأي اتفاق من شأنه تنظيم الاستخدام العسكري للفضاء الإلكتروني أن يعمل على منع نشر الأسلحة الإلكترونية في وقت السلم، والسماح بالجهود الجماعية للدول أو المنظمات لتجنب التأثير على الاستخدام المدني للفضاء الإلكتروني[١٣٨].

(١٣٧) والتي تضمنت ثلاثة مبادئ أساسية: ١- عدم حيازة الأسلحة النووية، ٢- عدم وضع الأسلحة النووية، ٣- عدم استخدام الأسلحة النووية.

(١٣٨) Misha Glenny, “A Weapon We Can't Control”, *The New York Times* (24 June 2012), online e-article, http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html?_r=0.



رابعًا: التغير في استراتيجية الردع من العصر النووي إلى الفضاء الإلكتروني

أ- الفضاء الإلكتروني والردع النووي:

مع زيادة القدرة على امتلاك القوة التكنولوجية بين أطراف دولية عديدة ازدادت معها القدرة على إحداث مستويات خاصة من الردع في مواجهة أطراف أخرى، ومن أهم تعريفات «الردع» بأنه «محاولة طرف ما ثني طرف آخر عن الإتيان بفعل يرى الطرف الأول أنه ضار به، أو يجده ضروريًا لمنع الطرف الآخر من أن يفكر بالقيام بعمل ما، أو الإتيان بتصرف أو سلوك معين يمكن أن يشكل تهديدًا لمصالحه أو لأهدافه أو لموقعه أو لمكانته».

وتعد نظرية الردع إحدى نظريات إدارة الصراع التي تستند أساسًا على الأدوات العسكرية، ويرتكز الردع على العامل النفسي والعقلي والعسكري، ويرتكن للقدرة وقابلية الانتقام. ويقوم الردع على أربعة مظاهر هي: الردع بالعقاب والردع بالحرمان والردع بالمكافأة والردع بالطمأنة، وعند محاولة تطبيق ذلك في إطار المجال الإلكتروني وأثره في تغيير نظرية الردع الاستراتيجية، وبخاصة فيما يتعلق بالردع النووي[١٣٩]، وبأن ارتباط العالم بمصالح مشتركة عبر الفضاء الإلكتروني قد عملت على ردع أي دولة أو قوى لممارسة القوة نتيجة لما سينتج عن هذا من تداعيات دولية. والعلاقة بين الفضاء الإلكتروني والطاقة النووية علاقة وظيفية، حيث تعتمد على الأدوات التقنية لتشغيل المفاعلات النووية عبر شبكات الاتصال والمعلومات وأجهزة التحكم الإشرافي. فقد نشأت بالأساس فكرة الإنترنت أو فيما بعد الفضاء الإلكتروني في محاولة لتفادي هجوم نووي على المنشآت النووية والعمل على تأمين الاتصالات، بالإضافة إلى علاقة تكنولوجيا بعمل المنشآت الحيوية كمحطات الكهرباء والطاقة والسدود والخدمات المدنية الأخرى. وقد أطلقت الأمم المتحدة تحذيرًا لحماية المنشآت النووية في العالم من خطر التعرض للهجمات الإلكترونية، وما يمكن أن تتسبب به من أخطار[١٤٠].

---

(١٣٩) Timothy Farnsworth, “Is there a Place for Nuclear Deterrence in Cyberspace?”, *Arms Control Now: The Blog of the Arms Control Association* (30 May 2013), online e-article, https://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace.

(١٤٠) وكان أبرز مثال على ذلك حالة استخدام فيروس ستكسنت كسلاح ضد المنشآت النووية الإيرانية، حيث عمل على تدمير ألف من أجهزة الطرد المركزي في مفاعل ناتانز الإيراني وذلك في أواخر عام ٢٠٠٩ وأوائل عام ٢٠١٠.

وعلى الرغم من استبعاد القدرة على شل البنية التحية الحيوية تمامًا في الوقت الحالي فإنه مرشح لإمكانية الحدوث في المستقبل القريب؛ وهو ما يتسبب في قلق متواصل من صانعي القرار والسياسات لدى الدول المختلفة، في سبيل وضع البدائل والحلول في مواجهة احتمال التعرض إلى الهجمات الإلكترونية. وفي ظل توجه الدول إلى تقوية قدراتها ليس فقط في مجال الدفاع في الفضاء الإلكتروني ضد الأخطار بل أيضًا الاستثمار في مجال الاستحواذ على القدرات الهجومية. ومدى ملائمة استخدام الأسلحة النووية للردع في مواجهة الهجمات الإلكترونية وهو ما لا يتناسب مع طبيعة الفضاء الإلكتروني، حيث يؤثر أي هجوم على دولة في دول أخرى وهو ما يشكل عقبة في سبيل استخدام الردع النووي.

إن فقدان السيطرة على الأمن في الفضاء الإلكتروني يمكن أن يؤثر في تشغيل عمل المفاعلات النووية وفي عمل الأسلحة الاستراتيجية وفي الأقمار الصناعية. وهو ما يتطلب البحث عن بدائل تدعم الدفاعات الإلكترونية وترفع درجات الاستجابة في حالة التعرض إلى مثل تلك الهجمات وبخاصة أن الرد بالأسلحة النووية ليس هو الحل الوحيد، فضلاً عن صعوبة تطبيقه أو استخدامه إلا أنه قد يستخدم لممارسة الضغط السياسي، وبخاصة مع وجود اتجاه عالمي إلى خفض استخدام الأسلحة النووية في ردع التهديدات غير النووية والذي كان قد بدا إبان الحرب الباردة بهدف خفض التوتر بين القوتين.

وأقرت محكمة العدل الدولية بعدم مشروعية استخدام الأسلحة النووية في حالة الدفاع الشرعي عن النفس. ضعف دور الأسلحة النووية في القيام بدور الردع الاستراتيجي مثل حالة التعرض للتهديدات الأمنية غير التقليدية مثل الكوارث الطبيعية أو نشاط الجماعات الإرهابية أو الإجرامية، وبالإضافة إلى الاتفاق الضمني على أن الأسلحة النووية يجب ألا تستعمل إلا لردع أي هجوم نووي. وانخفض دور الأسلحة النووية في ردع الهجمات غير النووية مثل الأسلحة التقليدية أو البيولوجية أو الكيماوية إلى جانب تقييد معاهدة منع الانتشار النووي لاستخدام أو التهديد باستخدام الأسلحة النووية ضد الدول غير الحائزة على الأسلحة النووية والمنضمة إلى المعاهدة. ومن ثم تصبح القدرة على التهديد باستخدام الأسلحة النووية للرد

على الهجمات الإلكترونية ليست واقعية، ولا تعبر عن استجابة فعالة للهجوم الإلكتروني، وذلك:

١- أن الهجمات السيبرانية - الإلكترونية تفتقر إلى التهديد الوجودي والمدمرة للأسلحة النووية.

٢- أن الرد بالأسلحة النووية على الهجوم الإلكتروني غير متناسب.

٣- أن التهديد بالرد بالأسلحة النووية يفتقر إلى المصداقية في أعين الخصوم.

٤- أن تحقيق الردع في الفضاء الإلكتروني بشكل عام من الصعب تحقيقه.

٥- أن من شأن تلك السياسة أن تشكل حافزًا وأساسًا منطقيًا للسعي إلى امتلاك الأسلحة النووية.

٦- هناك صعوبات في تحديد مصدر الهجمات، ومن ثم يصعب تحديد المسئولية عن تلك الهجمات.

٧- صعوبة التنبؤ بوقوع تلك الهجمات الإلكترونية بالإضافة إلى صعوبة معرفة الآثار الحقيقية التي تنتج عن مثل تلك الهجمات على الشبكات والبنية التحتية الحيوية. وتدفع تلك العوامل السابقة التي تشكل نقاط ضعف في مواجهة مخاطر عسكرة الفضاء الإلكتروني إلى أهمية البعد الدولي في مواجهة تلك الأخطار باعتباره مرفقًا عالميًا.

ب- الفضاء الإلكتروني ونظرية الردع الإلكتروني:

فرضت حرب الفضاء الإلكتروني نفسها على مقاربات الفكر الاستراتيجي العالمي، وباتت تشغل حيزًا كبيرًا من اهتمامات المخططين العسكريين والفكر الاستراتيجي، ويؤثر هذا التطور بشكل عميق الأثر على مقاربة مفهومي القوة والردع، ويعيد صياغة الكثير من



النظريات الخاصة بهذين المفهومين. والحاجة لإعادة بناء مفهوم التوازن الاستراتيجي برمته(١٤١).

وأصبحت مكونات الردع تتعرض للتأثير، سواء فيما يتعلق بالمقدرة على الانتقام، عبر الفضاء الإلكتروني نتيجة إلى الطابع العشوائي للهجمات الإلكترونية، والتأثير على إرادة الأطراف فيما يتعلق بحرية استخدام تلك القدرات في أوقات وظروف معينة.

وأصبح الضرر الناتج من استخدام الهجمات الإلكترونية يعطي نفس الأثر لاستخدام القوة العسكرية التقليدية، ولا يمكن لأي دولة أن تعرف حقيقة القدرات في مجال الحرب الإلكترونية أو مدى تطورها وبخاصة أنها لا تخضع لرقابة وليس لديها قابلية للتعرض لها. وبخاصة مع زيادة معدلات امتلاك القدرات في مجال الأسلحة الإلكترونية.

وشهد المفهوم الكلي لقوة الدولة تغيرًا كبيرًا في اللحظة التي ظهرت فيها حرب الفضاء الإلكتروني، وبات لزامًا على الدول المختلفة إعادة تقييم قوتها استنادًا لهذا المتغير. وعلى الرغم من تفوق الولايات المتحدة في القوات البحرية والجوية والفضاء فإنها أصبحت تواجه تحديات فيما يتعلق بالقوة الإلكترونية.

وتنفق الولايات المتحدة ٩٠ ٪ من ميزانية الحرب الإلكترونية على الدفاع، في حين أن ١٠ ٪ فقط مخصصة للهجوم، الأمر الذي يُضعف القوة الهجومية الأمريكية، وهو ما يشكل نقط ضعف استراتيجية في أمنها القومي. ورغم ذلك، ليس الوزن الكلي للقوة هو الأهم في إطار هذه المقاربة، إن البعد الأهم هو موقع الردع فيها.

ويهدف الردع الإلكتروني إلى القدرة على منع دولة، أو أفراد، أو منظمات غير حكومية، من شن هجوم إلكتروني ضد شبكات بيانات حكومية، أو بنى تحتية حيوية. وفي ظل الدفاع عن الأمن الإلكتروني والذي يجب أن يشتمل على حماية البنى التحتية الحيوية (الكهرباء، الغاز، الوقود، النقل، الاتصالات السلكية واللاسلكية، شبكات الطوارئ.. إلخ) والتي غالبًا

(١٤١) عبد الجليل زيد المرهون، «عصر الردع الإلكتروني»، **الجزيرة نت**، http://www.aljazeera.net/2FC311D7-4DFD-41E6-93FD-64B5C7A8C1D9/ForceRequestingFullContent/2FC311D7-4DFD-41E6-93FD-64B5C7A8C1D9/knowledgegate/opinions/2012/10/26/%d8%b9%d8%b5%d8%b1-%d8%a7%d9%84%d8%b1%d8%af%d8%b9-%d8%a7%d9%84%d8%a5%d9%84%d9%83%d8%aa%d8%b1%d9%88%d9%86%d9%8a.



ما تعتمد كليًّا على أنظمة التحكم والاتصال، واعتبرت روسيا أن السلاح الذكي يتحول إلى عامل استراتيجي أهم وأكثر فاعلية للردع غير النووي، حيث يجمع بين وسائل الاستطلاع والقيادة والنقل والتدمير.

وأحدثت تلك القدرات تغيرًا في مفهوم الردع التقليدي، وهو ما يعني أن أي دولة محدودة القدرات بالمفهوم الكلي للقوة، ولم تشهد تطورًا عسكريًّا لديها، وغير قادرة على بناء معادلة ردع نووي أو فوق تقليدي أو تقليدي يمكنها أن تفرض نفسها من خلال نوع جديد من الردع هو حرب الفضاء الإلكتروني. وفي اللحظة التي تنجح فيها في بناء قاعدة دفاعية وهجومية لهذه الحرب، الدول الأضعف والتي قد لا تمتلك قدرات هجوم عسكرية كبيرة وليست عضوًا في حلف عسكري؛ فإنه يمكن لها أن تنجح في بناء قاعدة متطورة لحرب الفضاء الإلكتروني وبأقل تكلفة وتوفر لها إمكانية شن هجمات على الأعداء.

وتشكل عملية التقدم في تلك القدرات في نفس الوقت ردعًا أمام أقدام أي دولة بمحاولة شن هجمات عليها أو قصفها بالأسلحة التقليدية. ويمكن أن تشن الدولة الأضعف في القدرات العسكرية التقليدية هجمات لتعطيل الشبكات الدفاعية واختراق النظم الصاروخية وشل منظومته الرادارية لدول كبرى بالإضافة إلى إمكانية الدخول على شبكة الدفاع الجوي، وإفساد نظم التحكم والسيطرة.

وتستخدم الدول القدرات في مجال الأسلحة الإلكترونية في خلق أزمات داخلية للنظام الحاكم أو بتدمير شبكات البنية التحتية المدنية للعدو، بما في ذلك شبكات الماء والكهرباء والطاقة النووية وسكك الحديد، والقطاعات الإنتاجية المختلفة، والمصارف وأسواق المال. ويمثل ذلك ردعًا من نوع جديد وفي بيئة مختلفة وبآليات غير مسبوقة في قدراتها في إصابة العدو أو في تطويرها والمزايا المتعلقة برخص تكلفتها، ومن ثم فإن الدول الصغرى والكبرى والمتوسطة أصبحت على قدم المساواة في تطوير مثل تلك الأسلحة الإلكترونية[١٤٢].

(١٤٢) James R. Hosek, "The Soldier of the 21st Century", Chapter 7 in *New Challenges, New Tools for Defense Decision Making*, edited by Stuart E. Johnson, Martin C. Libicki and Gregory F. Treverton (Santa Monica, CA: RAND, 2003): 196.



ويفرض ذلك عبئًا على الدول الكبرى أمام العمل على تعظيم قواه في مجال الأسلحة الإلكترونية، وبخاصة مع عدم القدرة على فرض الرقابة أو الحد من التسلح الإلكتروني، ويبقى الرد هو العمل على ممارسة الدبلوماسية من أجل إثناء أي دولة خصم في استخدام هذا النمط الجديد من التسلح، وبخاصة أن عملية استخدام تلك الأسلحة لا تستغرق وقتًا طويلاً ولا تحتاج تعبئة أو تدشين منصات لإطلاقها، وهو ما يجعل الدولة المستهدفة في حالة مستمرة من إمكانية التعرض للهجوم في وقت ودون سابق إنذار ومن جهات قد تبدو غير معلومة، ووجود مشكلة في إمكانية امتصاص الضربة الأولى وتأثيرها على إمكانية استعادة القوة مرة أخرى والرد على مصدر الهجمات.

وقد تؤدي الهجمات الإلكترونية على الدولة إلى تحسين نظم دفاعاتها الإلكترونية ومعرفة قدرات الخصم وتتمكن من توفير أسلحة هجومية، وهو ما جاء في حالة الهجوم الإلكتروني على إيران في عام ٢٠١٠ قد ساعد إيران على تطوير استراتيجية قومية للأمن الإلكتروني وفي مجال الحرب الإلكترونية على النحو الذي جعل إيران تحرز تقدمًا في تطوير الأسلحة الإلكترونية في زمن وجيز؛ لأن العبرة في امتلاك القدرات تتمثل في الخبرات في التعامل وإمكانيات البحث والتطوير.

ومن ثم فإن عملية شن هجمات من دولة إلى دولة أخرى قد يؤدي إلى رد فعل أقوى ومفاجئ لعدم توافر معرفة حقيقية عن حجم التسلح الإلكتروني ونوعياته وتطويره، وهو ما يجعل قدرات الخصم يكتنفها الغموض؛ وهو ما يسبب في ذات الوقت ردعًا لتعرض تلك الدولة للهجوم، وبخاصة مع توسيع دائرة الهجمات من خلال استهداف المنشآت العامة والخاصة بما يعمل على شلل أجهزة الدولة وليس فقط مهاجمة المنشآت العسكرية، وهو ما يفرض على الدول أن تشرك القطاع الخاص والمجتمع المدني في خطط واستراتيجية الأمن الإلكتروني.

وعلى الرغم من أهمية التعاون الدولي في مكافحة التسلح الإلكتروني فإن بعض الدول تخشى إتاحة التعاون الفرصة للكشف عن قدراتها أمام دول أخرى، وهو ما يدفعها إلى

محاولة إيجاد التوازن الحساس بين مصالحها الاستراتيجية وأسرارها الحساسة، لكي لا تُدخل هدفًا ذاتيًّا في مرماها(١٤٣).

ويأتي ذلك في ظل تحول القوة في عصر الفضاء الإلكتروني، والتي لم تعد تعتمد فقط على الدفاعات القوية للدولة بل من خلال المشاركة القوية مع الحلفاء، ويساعد هذا التشارك في تعزيز قدرة الآخرين على التعاون، وتقاسم المعلومات السرية والقدرات مع الآخرين، والتي تعمل على تحسين القدرة على التعامل مع التحديات الجديدة.

وتختلف عملية «الردع الإلكتروني» من حيث الآليات عن صيغة الردع النووي، والذي قد يستخدم الأخير لثني العدو عن شن أعمال هجومية مضادة من البداية، بينما يتيح الردع الإلكتروني إمكانية إبطال الأعمال الهجومية العدائية أو تحييدها بقدر الإمكان، وليس فقط منعها من البداية، وذلك بفضل ثلاثة عوامل: الأول، مزيج من الحماية الإلكترونية المتقنة والمتينة لحماية محيط شبكات المعلومات والبنية التحتية: الكهرباء والمياه والغاز والاتصالات السلكية واللاسلكية والنقل والصحة والموارد المالية والحكومة والشرطة والقوات المسلحة وغيرها ما يضمن إحباط أي هجوم.

والثاني، التعزيز المستمر والعمل على وجود وفرة دائمة لمعلومات هذه الشبكات والبنى التحتية ما يؤدي لتحديث هذه المعلومات بشكل دائم وصعوبة كشفها، الأمر الذي سيكون من شأنه الحد أو محو التأثير المتسلسل للهجمات التي تسببها الهجمات الإلكترونية.

والثالث، رصد ومراقبة نشاط مشغلي الأنظمة (من المعتدين المحتملين) في دوائر أمن الفضاء الإلكتروني، الأمر الذي سيعطي فرصة كافية لعمل هوامش لتحليل الأمر عن كثب، واعتماد الحماية المناسبة لهجمات متوقعة، وفقًا لتحليلات مدروسة تقيم المخاطر والأضرار.

ويركز الردع الإلكتروني في المقام الأول على زيادة المرونة في شبكات المعلومات الاستراتيجية والبنى التحتية الحيوية وعلى تحصينها بشكل متزايد، وفي المقابل، فإن هذا

(١٤٣) Tim Stevens, “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace”, *Contemporary Security Policy* 33, no. 1 (2012): 148-170.

سيثبت في النهاية للمهاجمين أن أعمالهم ستكون لها عواقب محدودة، وقد يثنيهم من البداية عن شن هجمات، ما يحقق أيضًا مبدأ الردع الاستباقي – في حالة النووي – وهو ما سيتطلب جهودًا ضخمة.

وهناك من يرى أن الردع لا يعمل في الفضاء الإلكتروني بسبب مصاعب تحديد المسئولية عن الهجمات، ومن ثم تحديد الطرف المهاجم، إلا أن عدم تحديد المسئولية بشكل كافٍ يؤثر على الردع بين الدول أيضًا، لكنه ما يزال يعمل. وحتى لو تم إخفاء مصدر الهجوم بشكل ناجح تحت «علَم زائف» فإن الحكومات يمكن أن تجد نفسها مشتركة في علاقات مترابطة ومتماثلة، مما يعني أن أي هجوم كبير ستكون له نتائج عكسية. إن المهاجم غير المعروف يمكن أن يرتدع إذا كانت هناك إجراءات مناسبة للأمن الإلكتروني. ولو كانت الجدران النارية قوية، أو كان التعزيز والمرونة يسمحان باستعادة النشاط بشكل سريع، أو توفرت الإمكانية لوجود رد ذاتي (سياج كهربائي)، فإن فكرة الهجوم تصبح أقل جاذبية.

وهناك صعوبة في تحديد مسئولية الهجوم الإلكتروني ومعرفة مصدره على الأقل في اللحظات الأولى لوقوع الاعتداءات الإلكترونية. وهو ما يجعل هناك صعوبة في تطبيق القانون الدولي، وإذا أخذنا بالاعتبار طبيعة الفضاء الإلكتروني، فذلك يعني أن الأمر يتطلب درجة من التعاون الدولي حتى يعمل.

ويطالب البعض بأن تكون هناك معاهدات تتعلق بالجانب الإلكتروني، والتي تعادل معاهدات الحد من الأسلحة. ولكن الفروقات في المبادئ الثقافية ومصاعب التحقق سوف تجعل من الصعوبة بمكان التفاوض على مثل هذه المعاهدات أو تطبيقها. وفي الوقت نفسه، فإن من المهم متابعة الجهود الدولية من أجل تطوير أسس للطريق الذي سوف يؤدي إلى الحد من الصراع. ولعل من جوانب التعاون الدولي الواعدة حاليًّا هي تلك التي تتعلق بالمشاكل التي تتعرض لها الدول بسبب أطراف أخرى من غير الدول، مثل المجرمين والإرهابيين.

يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في حروب الفضاء الإلكتروني، فالردع بالانتقام أو العقاب. في الحروب التقليدية ينطلق



الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة في كثير من الأحيان تحديد مصدر الهجمات الإلكترونية والفاعلين، وهو ما يلغي مفعول الردع بالانتقام وبخاصة إذا كانوا فاعلين من غير الدول. وتبقى أساليب الردع ضد الهجمات المحتملة في:

أ- جمع المعلومات عن الخصوم الحاليين والخصوم المحتملين، حتى لو كانوا أصدقاء حاليين.

ب- العمل على تطوير القدرة لدى الدولة في الردع العسكري والسياسي والاقتصادي، وتخفيف تأثير قدرات الخصم في الردع.

ج- العمل على تسريب معلومات تضخم قدرة الدولة في الردع لضمان تصور الخصوم بالتفوق في الردع.

خاتمة الدراسة

نحو خارطة طريق عالمية للتعامل مع الأسلحة الإلكترونية وتأمين الفضاء الإلكتروني

أولاً: الجهود الدولية في سبيل تأمين الفضاء الإلكتروني

لم ينصّ ميثاق الأمم المتحدة صراحة على تجريم استخدام حرب المعلومات أو الهجمات الإلكترونية؛ نظرًا لأن روح الميثاق تتفق مع تجريم استخدامه باعتباره يمثل انتهاكًا لما ورد في الميثاق بخصوص «التهديد أو استخدام القوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة». وقام عدد من الدول بالتركيز على الخصائص المدمرة للاستخدام غير السلمي للفضاء الإلكتروني وخطورة تحوله إلى ميدان حربي على نطاق عالمي، واتجهت العديد من الدول إلى اعتبار الفضاء الإلكتروني مجالاً خامسًا للحرب إلى جانب الأرض والجو والبحر والفضاء الخارجي. وقد أشارت دراسة لمعهد الأمم المتحدة لنزع السلاح في عام ٢٠١١ أن هناك ٣٣ دولة من ١٣٣ دولة عملت على تضمين الحرب الإلكترونية في تخطيطها العسكري والتنظيمي.

وفي يونيو ٢٠١٢ قام الأمين العام للأمم المتحدة بان كي مون بتشكيل لجنة خبراء جديدة تضم ١٥ عضوًا، منها خمس من الدول دائمة العضوية في مجلس الأمن، بالإضافة إلى الأرجنتين وأستراليا وبيلاروسيا وكندا ومصر وإستونيا وألمانيا والهند وإندونيسيا واليابان للتنسيق مع الجمعية العامة للأمم المتحدة حول دراسة إجراءات التعاون الممكنة لمواجهة الأخطار المحتملة المرتبطة بتكنولوجيا الاتصال والمعلومات[١٤٤]، وتقوم الأمم المتحدة بإعادة تشكيل تلك اللجنة في عام ٢٠١٤ لزيادة عدد أعضائها إلى ٢٥ عضوًا.

بالنظر إلى خصائص السلاح النووي غير التقليدية وآثارها التي تجعل استخدام هذه الأسلحة في الواقع يبدو كارثيًا بما يدعو إلى أن يتم التعامل معها وفقًا لتلك الاعتبارات

(١٤٤) "United Nations: Recent Developments in the Field of Information and Telecommunications in the Context of International Security", NATO Cooperative Cyber Defence Centre of Excellence: *Incyder News* (14 Nov 2012), online e-article, https://ccdcoe.org/united-nations-recent-developments-field-information-and-telecommunications-context-international.html.



القانونية التي يتمُّ التعامل بها في مثل تلك الحالات وفق القانون الدولي، والذي تعامل مع إخضاع السلاح النووي لقواعد النسبية والضرورة والوسطية والتمييز والحياد والإنسانية وحماية المدنيين[١٤٥].

وجاء رأي محكمة العدل الدولية أن التهديد باستخدام الأسلحة النووية أو استخدامها بالفعل يتعارض بشكل عام مع قواعد القانون الدولي التي تتعلق بحالة النزاعات المسلحة، وبالتحديد قواعد القانون الدولي الإنساني. ولكن بالنظر إلى الوضع الحالي للقانون الدولي فإن «محكمة العدل الدولية تذهب إلى القول بأن مبادئ وقواعد القانون الذي يتناول الصراع المسلح وبالنظر إلى روح وقلب مبادئ الإنسانية التي تجعل الأعمال المسلحة خاضعة لعدد من المطالب والشروط؛ لذلك فإن وسائل الحرب وطرقها التي ربما تعمل على إزالة التمييز ما بين المدنيين وغير المدنيين والأهداف المدنية والعسكرية أو النظر إلى ما قد يترتب على استخدامها من آلام أو أضرار لا مبرر لها للمحاربين.. تصبح محرمة»[١٤٦].

ويمكن لبعض التأثير الذي يتعلق بالأسلحة النووية أن يتشابه مع حالة الهجوم عن طريق استخدام أسلحة وهجمات الفضاء الإلكتروني، ويتمُّ في مثل هذه الهجمات تعرُّض كل البنية التحتية الكونية للمعلومات لخطر الدمار والتعطيل، بما يكون له من أثر على الدولة التي تكون ضحية لتلك الاعتداءات، وأيضًا ما يتصل بتهديد المجتمع الدولي ككل عن طريق شبكات الاتصال والمعلومات التي تربط دول العالم بعضها ببعض، وتزايد درجات الاعتماد المتبادل بين دول العالم، وما ينتج عن ذلك من انتهاك لقيم ومبادئ القانون الدولي الذي عمل على إرساء الاستخدام السلمي والتعاون والتفاهم بين شعوب العالم.

---

(١٤٥) Foreign and International Law Committee of the New York County Lawyers'Association "NYCLA", *Report of the Foreign and International Law Committee of the New York County Lawyers' Association on the Unlawfulness of the Use and Threat of Use of Nuclear Weapons* (New York, 2000), online e-report, http://www.nuclearweaponslaw.com/JournalsReport/NYCLA_Report.pdf.

(١٤٦) تُعد محكمة العدل الدولية منظمة منبثقة عن الأمم المتحدة وأنشئت بموجب ميثاقها في عام ١٩٤٥ وبدأت عملها في إبريل عام ١٩٤٦ ويوجد مقرها في لاهاي، وللمزيد عن رأيها الاستشاري حول استخدام السلاح النووي في النزاع المسلح في عام ١٩٩٤، انظر: **محكمة العدل الدولية**، http://www.icj-cij.org/homepage/ar ؛ وكذلك الاطلاع على:
"Legality of the Use by a State of Nuclear Weapons in Armed Conflict", Advisory Opinion. *International Court of Justice*. http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4&case=95.

وبخاصة مع تصاعد استخدام الأسلحة الإلكترونية وحالة السباق العالمي حول الاستحواذ على مقدراتها بما يعمل على تهديد أمن الفضاء الإلكتروني، بالإضافة إلى الاستخدام غير السلمي للفضاء الإلكتروني من قِبل الجماعات الإرهابية أو جماعات الجريمة المنظمة والقراصنة وغيرها، ما يمثل انتهاكًا للطابع السلمي للفضاء الإلكتروني، ويتم تطوير تلك الأسلحة بدون أي تكاليف مادية باهظة، وهناك توافر لمصادر المعرفة الكاملة عنها عن طريق ما يتم تداوله عبر مواقع الإنترنت؛ حيث تتم إتاحة معلومات عن القراصنة والاختراق وسرقة المعلومات وفكّ التشفير وضرب البرامج وغيرها.

ويمكن لأي فرد أن يتعلمها سواء بدافع ذاتي أو عن طريق توظيفه من قِبل فاعلين من غير الدول. وهذا ما يظهر في انتشار تلك الأسلحة أو نقلها واستخدامها وتخزينها وعدم خضوعها للرقابة مقارنة بحال الأسلحة النووية[١٤٧]. وهذا ما يُدخل عملية استخدام تلك الأسلحة عبر الفضاء الإلكتروني ضمن الهجمات المتعمدة والعشوائية وغير المتناسبة التي تسبب الأضرار للمدنيين، فهي لدى ارتكابها بقصد إجرامي، تُعتبر جرائم حرب. ويمكن أن يصبح الأشخاص القائمون عليها عرضة أيضًا للمسئولية الجنائية في إطار ارتكاب جريمة حرب، وكذلك ما يتعلق بالمعاونة فيها أو تسهيلها أو المساعدة على ارتكابها أو الحثّ عليها[١٤٨].

وأنه لا يوجد موقف دولي واضح من هجمات الفضاء الإلكتروني ولا توجد سوابق قانونية يمكن الاستناد إليها، وهذا ما يدفع إلى ضرورة الوصول إلى نظم قانونية يمكن أن تنشئ قواعد خاصة بتنظيم استخدام الفضاء الإلكتروني وتجريم استخدامه في الأغراض العسكرية، أو تلك الأنشطة التي تضرُّ بأهميته ودوره في المجتمع الدولي. وهذا ما يتطلب أهمية الوصول إلى اتفاقية دولية شاملة حول الأمن الإلكتروني. ويمكن أن تتم معاملة الأسلحة

(١٤٧) وبلغ ذلك إلى حد تشبيه أسلحة الفضاء الإلكتروني بأسلحة الانتشار الشامل على نسق أسلحة الدمار الشامل، حيث انتشار وإتاحة إمكانية امتلاكها واستخدامها ونقلها وتطويرها بدون تكلفة كبيرة، بما يمكن أن يتيح ذلك للدول الصغرى والجماعات الإرهابية والأفراد من تطويرها واستخدامها كوسيلة لتحقيق أغراض سياسية أو إجرامية أو غيرها.

(١٤٨) N.C. Rowe, "War Crimes from Cyber-Weapons", *The Journal of Information Warfare* 6, no. 3 (Dec 2007):15-25.



الإلكترونية، وما قد ينتج عن استخدامها في حالة الدفاع الشرعي أو في النزاع المسلح في إطار الأضرار الجسيمة التي تلحق بالمجتمع الدولي.

وأنه بالنظر إلى هجمات وأسلحة الفضاء الإلكتروني وموقف المحكمة الجنائية الدولية[١٤٩] باعتبارها شكلاً من أشكال العدوان، ويمكن أن تخضع هجمات الفضاء الإلكتروني لاختصاص هذه المحكمة فيما اعتبرته المحكمة جرائم إبادة جماعية، والتي تعني أي فعل يُرتكب بقصد إهلاك جماعة أو إلحاق ضرر جسدي أو إخضاعه عمدًا لأحوال معيشة مزرية. وهذا ما قد ينتج إذا ما تعرضت دولة ما أو مجتمع إلى الحرمان من الحصول على الخدمات أو تدمير البنية التحتية للمعلومات، مما يؤدي إلى أضرار اقتصادية جسيمة من جراء التعرُّض لهجمات الفضاء الإلكتروني. أما عن توصيف جرائم ضد الإنسانية والتي تعني أي هجوم أو فعل يُرتكب ضمن إطار هجوم واسع النطاق موجَّه ضد أي مجموعة من السكان المدنيين. ويظهر ذلك في حالة شنِّ هجمات الفضاء الإلكتروني التي تتميز بالانتشار الواسع عبر شبكات الاتصال والمعلومات والحرمان من الحرية للأفراد.

ويمكن اعتبار هجمات الفضاء الإلكتروني تقع ضمن مجموعة جرائم الحرب؛ حيث إنها تمثل إذا ما تم القيام بها انتهاكًا لاتفاقيات جنيف وما تتضمنه من حظر القيام بالتسبب في معاناة شديدة أو إصابات خطيرة بالجسم أو الصحة، أو تدمير الممتلكات والاستيلاء عليها، أو توجيه هجمات ضد السكان والمنشآت المدنية التي ترتبط في عملها بالفضاء الإلكتروني. ومن ثم فإن المسئولين عن تلك الهجمات يمكن اتهامهم بارتكاب جرائم حرب.

كما تُعَدُّ هجمات الفضاء الإلكتروني نوعًا من العدوان، على الرغم من عدم الاتفاق حول تعريف واضح له. إلا أن قرار الجمعية العامة للأمم المتحدة في ١٤ من ديسمبر من العام ١٩٧٤ أقرَّ بأن العدوان هو «استعمال دولة ما، القوة المسلحة ضد دولة أخرى ضد السيادة وسلامة الأرض والحرية السياسية أو بأي طريقة أخرى». وبالقياس على استخدام أسلحة

(١٤٩) منظمة دولية دائمة أنشئت عام ٢٠٠٢، تسعى إلى وضع حد للثقافة العالمية المتمثلة في الإفلاتِ من العقوبة، وهي ثقافة قد يكون فيها تقديم شخص ما إلى العدالة لقتله شخصًا واحدًا أسهل من تقديمه لها لقتله مائة ألف شخص مثلاً، فالمحكمة الجنائية الدولية هي أول هيئة قضائية دولية تحظى بولاية عالمية، وبزمن غير محدد، لمحاكمة مجرمي الحرب ومرتكبي الفظائع بحق الإنسانية وجرائم إبادة الجنس البشري.

الفضاء الإلكتروني، نجد أنها تمثل نوعًا من استخدام القوة ذات الطابع المرن أو الإلكتروني التي ينتج عن استخدامها غير المشروع نتائج استخدام القوة بمفهومها التقليدي نفسها.

ومن ناحية أخرى تأتي أهمية الجهود والمبادرات الدولية من قبل كافة الفاعلين في مجتمع المعلومات العالمي من أجل الحفاظ على الطابع السلمي للفضاء الإلكتروني، وبخاصة أن تعاظم التهديدات جعله يدخل في أولويات الأجندة الدولية وعلى رأس أولويات السياسة الخارجية للعديد من الدول وضمن استراتيجيات الأمن القومي لديها، ودفعت التهديدات المتزايدة لأمن الفضاء الإلكتروني العديد من الدول للعمل على بذل الجهود فرادى وجماعات بشأن الحفاظ على أمن الفضاء الإلكتروني سواء أكان متمثلاً في إنشاء هيئات لمواجهة الطوارئ المعلوماتية CERT أو استحداث قوانين لمكافحة الجريمة الإلكترونية أو بإنشاء قيادة عسكرية لحماية الفضاء الإلكتروني أو استحداث وحدات للحرب الإلكترونية داخل الجيوش العسكرية، أو المشاركة في مناورات إلكترونية لتحسين القدرات الدفاعية أمام الهجمات الإلكترونية[١٥٠].

هذا إلى جانب إطلاق العديد من المبادرات التي تقوم بها المنظمات الحكومية وغير الحكومية لدعم الأمن الإلكتروني مثل الاتحاد الدولي للاتصالات الذي أطلق مبادرة للأمن الإلكتروني، وحلف شمال الأطلنطي الذي أنشأ وحدة للدفاع الإلكتروني. وأطلق الاتحاد الأوروبي مبادرة للأمن الإلكتروني، وتبنت الولايات المتحدة «الاستراتيجية الدولية للفضاء الإلكتروني»، وهي أول وثيقة سياسية من هذا النوع تبين الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالفضاء الإلكتروني[١٥١].

وقد سعت عدد من الدول الأوروبية فيما عرف باسم ترتيبات فاسينار في الأسبوع الأول من شهر ديسمبر ٢٠١٣، بالعمل على وضع ضوابط حول تصدير تكنولوجيات التجسس وذلك في جنيف بسويسرا، وتمت إضافة فئتين جديدتين تتعلق بأنظمة المراقبة والتجسس

---

(١٥٠) عبد الصادق، **الإرهاب الإلكتروني: القوة في العلاقات الدولية**: ١٥٠–١٥٢.

(١٥١) Jefferson D. Reynolds, "Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground", *Air Force Law Review* 56 (2005): 1-108.



ووضعها في قائمة السلع والتكنولوجيات ذات الاستخدام المزدوج، وهو ما يشكل اعترافًا للمرة الأولى بضرورة إخضاع أدوات التجسس والأسلحة الإلكترونية التي تستخدمها وكالات الاستخبارات وتنفيذ القواعد القانونية التي تنظم ضوابط التصدير إلى دول أخرى.

ومن شأن الجهد الدولي للتعامل مع الأسلحة الإلكترونية والتي لها قدرة على الانتشار الشامل عبر الفضاء الإلكتروني، أن يرتكز على ثلاثة التزامات أساسية وهي: الأول، العمل على اتخاذ وتنفيذ تدابير فعالة لوضع ضوابط لمنع انتشار الأسلحة الإلكترونية ووسائل استخدامها. والثاني، الامتناع عن تقديم الدعم للجهات الفاعلة من غير الدول التي تحاول استحداث أو اقتناء أو صناعة أو امتلاك أو نقل أو تحويل أو استعمال الأسلحة الإلكترونية. والثالث، العمل على اعتماد وتنفيذ قوانين مناسبة وفعالة لحظر صناعة أو اقتناء أو امتلاك أو تطوير أو استعمال الأسلحة الإلكترونية.

وذلك في إطار: الاعتبار الأول، موقف القانون الدولي من أسلحة حديثة لم تتم الإشارة إليها في قانون الحرب بالتجريم أو بشكل محدد. والاعتبار الثاني، إنه تم التوافق ما بين طبيعة تلك الأسلحة والمبادئ العامة التي كان من شأنها تجريم استخدامها الأسلحة الأخرى بموجب القانون الدولي. والاعتبار الثالث، يعد ذلك سابقة تاريخية تدخل في إطار العرف الدولي، ويمكن أن يتم تطبيقها على أي أسلحة يكون من شأنها إحداث ذلك الضرر أو الأثر بالمجتمع الدولي يخالف قواعده العامة.

ومن الملاحظ أن سباق الاستحواذ على الأسلحة الإلكترونية في حرب الفضاء الإلكتروني يكتنفه الغموض بعدم رغبة الأطراف أو قدرة طرف آخر على معرفة حقيقة امتلاك تلك الأسلحة، وأن استخدام تلك الأسلحة يتم بسرعه فائقة يصعب قياس حجم الأضرار أو معرفة نوعية الأسلحة المستخدمة إلا بعد الاستخدام، وهو ما يفرض تحديًا أمام صناع القرار بشأن الحرب أو في الحزم بشأن القدرة على الدفاع. إن هجمات الحرب في الفضاء الإلكتروني تأخذ شكلاً عالميًّا متسعًا في نطاقها باتساع الفضاء الإلكتروني وتعدية للحدود الدولية، اللهم إلا التقدم في مجال تطوير أسلحة إلكترونية تستخدم في نطاق جغرافي معين أو ضد منشآت بعينها، ولكن البعد العالمي للهجمات يساعد في اتساع نطاق



التأثير للعدوان الإلكتروني .وترتكز قدرات الدول في الدفاع والهجوم ليس على القدرات في امتلاك الأسلحة التقليدية أو أسلحة الدمار الشامل، بل القدرة على التحكم والسيطرة في النظم المعلوماتية للمنشآت الحيوية، وهو ما يعمل على تغيير موازين القوة لدى الدول الكبرى. لا يمكن فصل ذلك السباق حول امتلاك الأسلحة الإلكترونية بمعزل عن الطبيعة الجديدة للمجتمع الدولي الذي أصبح أكثر ارتباطًا بالتكنولوجيا وتشكل عصبه الجديد، وكذلك يجب الأخذ بعين الاعتبار أن طبيعة الصراعات والتحالفات على الأرض لها انعكاس على طريقة تعامل الدول مع قدرات الفضاء الإلكتروني.

وهو ما عكس صعوبة قوة الدولة في مجال حرب الفضاء الإلكتروني من ناحية القدرات الدفاعية أو الهجومية، وعلى المجتمع الدولي بكافة الفاعلين في مجتمع المعلومات العالمي سواء كانوا حكومات أو مجتمع مدني أو أكاديمي أو قطاع تقني وشركات تكنولوجي العمل سويًّا للعمل على الحفاظ على أمن الفضاء الإلكتروني. وقيام الأمم المتحدة بإدخال الأمن الإلكتروني ضمن اختصاصات مجلس الأمن الدولي وباعتباره على رأس الأجندة الدولية وتحت رعاية أممية. والعمل على تضافر الجهود لإقامة حوار بناء بين الدول الكبرى حول حدود استخدام الأسلحة الإلكترونية في الصراعات الدولية، ومنع تصدير التكنولوجيا المتقدمة إلى مناطق الصراع وأطرافه المختلفة وتكوين لجنة خبراء عالمية لإدارة الأزمات الإلكترونية الدولية، والعمل على تطوير اتفاقيات الحد من التسلح أو تطوير إجراءات السلامة عبر العديد من المنظمات الدولية المعنية وتعزيز دور الإعلام والصحافة في التحذير من خطورة البيئة غير الآمنة في الفضاء الإلكتروني. وسن قوانين وتشريعات تواجهه الجريمة الإلكترونية وتطوير منظمة الأمن الإلكتروني، وإلى جانب أهمية مراعاة البعد الاجتماعي والاقتصاد لعناصر الخطر للأمن في الفضاء الإلكتروني بمواجهة عالمية للفقر والبطالة وحل وتسوية الصراعات الدولية.

ثانيًا: نحو اتفاقية دولية لحماية وتأمين الاستخدام السلمي للفضاء الإلكتروني

أصبح هناك قواعد للقانون الدولي تنطبق مباشرة على أنشطة الفضاء الإلكتروني، تتمثل في: المبادئ المعمول بها بين الأمم، مبادئ القانون الدولي الناشئة عن القانون الدولي العرفي والمعاهدات، المبادئ العامة التي استندت إليها الأمم المتحضرة كـ: القواعد التي تحكم اللجوء لاستخدام القوة، قواعد التسوية السلمية للمنازعات الدولية، القواعد المحدِّدة لقواعد الدفاع عن النفس، القواعد المتضمَّنة في ميثاق الأمم المتحدة والنظام الأساسي لمحكمة العدل الدولية والقانون الدولي الإنساني.

وهناك نوعان من القواعد القانونية: الأول يعمل على إشباع الحاجات والمصالح العليا والمشتركة للمجتمع الدولي ككل، وهي قواعد مطلقة في تطبيقها. وهناك أيضًا القواعد النسبية التي تنظم حقوق الدول وواجباتها فيما بينها، ولا تسري إلا فيما يتعلق بهذه الحقوق أو تلك الواجبات.

تطرح طبيعة هجمات الفضاء الإلكتروني مدى إمكانية تطبيق القواعد القانونية الدولية التي تنبثق من ميثاق الأمم المتحدة، وهي تساعد على المعالجة القانونية، فضلاً عن أن الأطر القانونية ليست كافية للتوصل إلى حلول تعالج معضلة الأمن التي تفرضها هجمات الفضاء الإلكتروني. وهناك وجهتا نظر في هذا الخصوص، الأولى منهما ترى أن هناك حاجة إلى وجود إطار قانوني جديد كلي، أما وجهة النظر الأخرى فترى الاقتصار على تبني النظم القانونية القائمة فقط. ولا شك أن أفضل طريقة لضمان معالجة شاملة تكمن في وجود اتفاق دولي يتعامل بالتحديد مع الأمن الإلكتروني وكيفية وضعه وطريقة معالجته في القانون الدولي. وتطرح أفضل طريقة لكيفية إنشاء بيئة قانونية تنظر إلى العدوان الإلكتروني باعتباره إخلالا جسيمًا بالنظام القانوني ومرادفًا للجريمة الدولية المنظمة أو عدوانًا ضد دولة أخرى.

وتدفع عملية الضرر المتوقع والمتخيَّل في حالة التعرُّض لهجمات الفضاء الإلكتروني إلى إثارة الجدل بشأن إمكانية تطبيق ما أرساه القانون الدولي الإنساني من قواعد تعمل على الحدِّ من استخدام القوة أو التهديد بها أو حتى تنظيم استخدامها في حالة الصراعات

المسلحة الدولية وغير الدولية الطابع، بهدف حماية المدنيين والمنشآت المدنية والأماكن التي تستحق حماية خاصة أو المنشآت التي تحتوي على خطورة خاصة. والخطرُ لم يَعُدْ مقتصرًا فقط على مصالح الأمم أو جماعات الضغط. وإنما يكمن الخطر الأساسي الذي يمكن أن ينتج عن «الحضارة العالمية» في الحدِّ من التعدد ومن إمكانات الاعتراف بالآخر، وذلك من خلال تنميط أشكال التعامل. وبمعنى آخر، فإن تحقيق الشفافية وتسهيل تداول المعلومات على المستوى العالمي يتمُّ على حساب الاختلاف والتعدد. فمستوى حضارة ما يُقاس من خلال درجة احتوائها على ما لا يمكن توقعه.

إن وحدة الإنسانية لا يمكن بأي شكل من الأشكال أن تتأسس على وحدة الدين أو الفلسفة أو السلطة، بل يكمن شرط تحققها أساسًا في التعددية. وتبقى مسائل التعاون الدولي لها أهمية بالغة، أبرزُها الاتفاق في حقل الاختصاص القضائي والقانون واجب التطبيق في بيئة النزاع في الفضاء الإلكتروني، وهذا ما يتطلب معرفة الأسس التي يتعين أن يتمَّ التفكير فيها في كل نشاطٍ يهدف إلى تنظيم ضروري للفضاء الإلكتروني. والأهم أن يكون تنظيمًا يراعي هذه السمات التقنية وهذه الخصائص والمميزات التفاعلية اللامتناهية.

يعبر الفضاء الإلكتروني من دولة لدولة ومن منطقة إلى أخرى، ومن جهة عمل إلى أخرى دون قيود وبكل اللغات، مع التداخل بين الشبكات المحلية والإقليمية والدولية. وفي هذا الانتقال يتمُّ المرورُ عبر مناطق الاختصاص القضائي ومناطق السيادة في العالم. وهذه المناطق قد لا يكون بينها تعاون أو حتى روابط، ففي مثل هذه البيئة ثمة حاجة لجهد استثنائي على النطاق الدولي أهم ما يتعين أن يتصف به: الخروج من الأطر والمفاهيم التقليدية التي بُني عليها القانون الدولي.

والعمل على اتخاذ تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية، مع وجود اتفاقيات دولية تنطوي على نصوص تنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، وأيضًا الأشكال الأخرى للمساعدة المتبادلة، مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول. وتُعَدُّ التعاملات المرتبطة بتقنية المعلومات

كغيرها من مجالات الحياة واجبة الخضوع للأحكام المستمَدة من القانون الدولي والعرف، بما يكفل وضع الحقوق والتزامات الأطراف المختلفة والموقف من القضايا المختلفة وفضّ النزاعات الناتجة عنها. وتُعَدُّ مسألة حماية البنية التحتية الكونية للمعلومات من ضمن أسس الأمن الدولي الجديد. ويتطلب ذلك: توافر قاعدة للتعاون الدولي المشترك، وتحديد ماهية تلك القطاعات الحيوية، مع توفير نظم حماية منتظمة لها، ودعم مواجهة الأخطار التي يمكن أن تتعرض لها على كل من المستوى التشريعي والسياسي والاجتماعي والاقتصادي، وأهمية دور الفضاء الإلكتروني في عمل البنية التحتية وما يلزمه من تعزيز الاستخدام السلمي له.

بذل المجتمع الدولي العديد من الجهود لحظر استخدام أسلحة الدمار الشامل والتقدُّم في شأن المناطق الخالية من السلاح النووي. وكما كانت العلاقة حميمية بين الأسلحة والتقدم التكنولوجي، فإنها أفرزت ثورة في الشئون العسكرية. وكان من ضمن ذلك: ظهور أسلحة الفضاء الإلكتروني التي أصبح لها أضرار، سواء من خلال تهديدها لأمن الفضاء الإلكتروني أو سعي الدول وغير الدول إلى تطويرها واستخدامها وانتشارها، بما يعيد إلى الأذهان الجهود الدولية لحظر أسلحة الدمار الشامل. وأصبح هناك إمكانية لتوظيف تلك الأسلحة التي تختلف عن الأسلحة التقليدية.

وأبرزت تهديدات تلك الاستخدامات على الطابع المدني للفضاء الإلكتروني الحاجة إلى تضافر الجهود الدولية من أجل العمل على تعزيز الأمن والحماية لدور الفضاء الإلكتروني الإيجابي على السيادة الدولية. وكان من ضمن تلك الجهود: الدعوة إلى اتفاقية دولية للحدِّ من التسلح داخل الفضاء الإلكتروني مثل تلك الاتفاقيات التي تم إنجازها في مجال الانتشار النووي والكيماوي والبيولوجي؛ حيث يمكن أن تسهم مثل تلك الاتفاقيات في حال تطبيقها على الفضاء الإلكتروني والأسلحة التي يمكن أن تُستخدم من خلالها في وضع قيود على استخدامها وتوزيعها وانتشارها وتطويرها.

ويمكن أن تخضع تلك الانتهاكات إلى القانون الجنائي الدولي ومحكمة العدل الدولية، ولكن ذلك يتطلب موافقة الدول. بيد أن عملية الدعوة إلى مثل تلك الاتفاقيات تواجَه بعدد من التحديات؛ حيث إن الدول قد ترفض الموافقة على أساس أن هذه القيود من شأنها أن

تحدَّ من قدرتها على تطوير الأسلحة الهجومية، وفي الوقت نفسه تحدُّ من قدرتها على الدفاع في حال التعرُّض لهجوم إلكتروني من دول أخرى أو فاعلين آخرين. كما أن ذلك الاتفاق يشمل فقط الدول، في حين أن عملية استخدام أسلحة الفضاء الإلكتروني يمكن أن تأتي من أطراف من غير الدول كالمنظمات الإرهابية والإجرامية التي لا تخضع لمثل تلك القيود.

إن تلك القيود التي قد تفرضها الاتفاقية على الدول من شأنها أن تعظِّم من قدرة الفاعلين من غير الدول على استخدام تلك الأسلحة في مقابل قدرات الدول. وهناك صعوبة في وضع الدول تحت الرقابة الفنية لقدرتها على تطوير أسلحة الفضاء الإلكتروني، وصعوبة في معرفة مصادر الهجمات (إن وقعت) وتحديد المسئولية بشأنها.

ويمكن أن تتعرض دول إلى اعتداء أو هجوم صادر من أجهزة حكومية في دولة أخرى، ولكن قد يحرك تلك الهجمات طرف ثالث يمكن أن يسيطر على تلك الأجهزة. وتتميز تلك الأسلحة بقدرتها الهائلة على الانتشار عبر الفضاء الإلكتروني، ومن ثَمَّ فإن نموذج منع الانتشار الخاص بالأسلحة النووية قد لا يصلح نموذجًا للتعامل مع الأسلحة في الفضاء الإلكتروني؛ ذلك لأن انتشار التكنولوجيا أصبح عالميًّا في المجتمع الدولي.

ومن ناحية أخرى أصبحت هناك صعوبة في الفصل بين الاستخدام المدني والآخر العسكري. وأن تحقيق الأمن الإلكتروني الجماعي الدولي يتطلب: أن يوجد إيمان وثقافة عالمية بأن السلام أمر غير قابل للانقسام أو التجزئة، مع ضرورة اتساع نطاق عضوية الدول فيه، وأن يكون ذلك النظام حياديًّا وموضوعيًّا، وأن توجد قوة عسكرية رادعة لردع المخالفين لذلك النظام. كما ينبغي أن يتركز على الناس وليس حول الدول بالضرورة. وهناك حاجة لوجود هوية إنسانية عالمية، مع احترام حرية الأفراد في أن تكون لهم هويات وانتماءات متنوعة، وضرورة تشكيل تحالف عالمي لتعزيز السياسات المؤسسية التي تربط ما بين الأفراد والدول.

ولكي يتم خضوع الفضاء الإلكتروني للقانون الدولي فإنه يحتاج إلى تغيير تنظيمي قانوني وسياسي وأمني وثقافي شامل. وأنه لكي يتمَّ التوصل إلى اتفاق دولي يجب أن يتمَّ



إطلاق حوار دائم حول ما يُعَدُّ جريمة وإرهابًا وما يمكن أن يدخل ضمن الاستخدام السلمي وأن يتم التمييز بينهما. وهذا الحوار يمكن أن يتقدم على جبهتين: الأولى، طبيعة الهدف الذي يمكن أن يدخل ضمن ضوابط وقواعد قانونية؛ وذلك لأنه يمثل أهمية ومعاناة لغير المحاربين كالهجوم على محطات الطاقة. أما الجبهة الثانية فهي طبيعة الأهداف التي تخرج عن الأطر القانونية والتي تصبح في حاجة إلى الحماية؛ حيث تكون إصاباتها غير معروفة ولا يمكن التنبؤ بنتائجها ولكنها تتسبب في حدوث معاناة.

ومن ثمَّ فإنه لكي يتمَّ التوصل إلى نظام قانوني دولي يحكم ظاهرة الفضاء الإلكتروني يجب أن يتم تحديد: (١) ماهية وكيفية التغلب على العمليات العسكرية باستخدام هجمات الفضاء الإلكتروني، (٢) أن تكون الاتفاقية قادرة على تحقيق التوازن بين مبدأين أساسيين هما: مبدأ الضرورة العسكرية، مبدأ احتمالية الوقوع، (٣) التمييز بين الأهداف العسكرية والمدنية، (٤) التصديق على هذه المعاهدة من المحكمة الجنائية الدولية. حتى يتمَّ تفعيل القانون الدولي لكي يتلاءم مع تلك الظاهرة.

ويحكم حركة تفاعلاتها يجب أن يستند إلى: (١) وسائل المنع أو الوقاية التي تُستخدم في تطبيق أحكام القانون الدولي لصالح الضحايا أو يتم تطبيقها تطبيقًا سليمًا، (٢) وسائل للرقابة، وهي وسائل الإشراف المتواصل بما يتضمن الالتزام السليم عند تطبيق الأحكام التي تتكفل بمصلحة الضحايا، (٣) العقوبات، وهي جزء لا يتجزأ من أي نظام قانوني سليم وذلك بسبب قيمتها الرادعة، (٤) ضرورة البحث عن وسائل أخرى كالأبعاد الاقتصادية والأمنية والثقافية[١٥٢].

(١٥٢) عادل عبد الصادق، **الإرهاب الإلكتروني: القوة في العلاقات الدولية**: ٤١١–٤٢٠.

التوصيات

يمكن تقديم عدد من التوصيات المتعلقة بكيفية الحد من التأثيرات السلبية لنمو التوجه العالمي في مجال تطوير واستخدام الأسلحة السيبرانية:

١– ضرورة العمل على تضمين الأسلحة السيبرانية في مجال اتفاقيات الحد من التسلح، وأن يتم التوصل إلى اتفاقية خاصة بالحد من الأسلحة السيبرانية على نحو ما تم في حالة أسلحة الدمار الشامل.

٢– العمل على إدخال المجال الإلكتروني ضمن استراتيجية الأمن القومي للدول، وتبني سياسات تتعلق بكيفية الاستحواذ على الأمن في مجال الفضاء الإلكتروني.

٣– العمل على تحديث الجيوش الحديثة بتقنيات ومهارات التعامل مع التهديدات السيبرانية، وكيفية الدخول في مجال الثورة في الشئون العسكرية، ويتم ذلك من خلال التدريب وإنشاء وحدات متخصصة في مجال الحرب الإلكترونية – السيبرانية.

٤– ضرورة التحرك على نحو جماعي للعمل على إدخال الفضاء الإلكتروني ضمن منظومة الأمن الجماعي الدولي، وأهمية أن يكون للمجتمع الدولي دور في العمل على الحفاظ على الطابع السلمي للفضاء الإلكتروني.

٥– يمكن أن تشكل إمكانية التوصل إلى اتفاقية دولية حول الفضاء الإلكتروني قوة دولية في مجال الدبلوماسية للعمل على الحفاظ على أمن وسلامة الفضاء الإلكتروني

٦– أهمية إدخال كافة أصحاب المصلحة في مجتمع المعلومات العالمي في تحمل المسئولية والمشاركة في حماية أمن الفضاء الإلكتروني، عن طريق إدخال الشركات الخاصة والحكومات والمجتمع المدني والأكاديمي والإعلام والنشطاء في استراتيجية رفع الوعي بمخاطر استخدام الأسلحة السيبرانية على الأمن الدولي.

٧– أهمية تفعيل المنتديات العالمية لحوكمة الإنترنت كمنصة دولية مفتوحة للجميع للنقاش حول الاتجاهات الحديثة في حماية الاستخدام السلمي للفضاء الإلكتروني.

٨– أهمية العمل على المستوى الدولي في حل الصراعات الدولية؛ حيث إن ما يحدث في المجال الإلكتروني انعكاس لحالة التوتر على الأرض، ومن ثم فإن خط المواجهة الأول يجب أن يكون العمل على حل وتسوية الصراعات بالطرق السلمية.

٩– أهمية قيام الدول على تحديث أطرها التشريعية لمكافحة الجريمة الإلكترونية لاحتواء المخاطر الداخلية على أمن الفضاء الإلكتروني.

١٠– أهمية العمل على تأمين البنية التحتية الكونية للمعلومات وإدخالها ضمن المنشآت المدنية المحظور استهدافها من قبل أطراف الصراع في حالة الحرب.

١١– أهمية إنشاء لجنة دولية لإدارة الازمات السيبرانية من خلال دراسة الهجمات الإلكترونية، والعمل على التحقيق الدولي المستقل حول المسئولية حول تلك الهجمات.

١٢– إنشاء مراكز تدريب محلية في مجال مكافحة الطوارئ المعلوماتية، والعمل على بناء القدرات في مجال الأمن الإلكتروني.

١٣– أهمية تعزيز التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وأهمية العمل على تعزيز التعاون في النظم القضائية وتبادل الخبرات.

١٤– أهمية دور المجتمع المدني العالمي في رفع الوعي بمخاطر الاستخدامات غير السلمية على الاقتصاد العالمي والأمن العالمي.

١٥– إن العمل على تنمية ثقافة عالمية تستهدف الفرد داخل الدول وعلى نطاق عالمي من المهم في درء المخاطر، وتجنب الاستخدامات الخطرة على أمن المجتمع والدولة.

١٦– أهمية تعاون الشركات التكنولوجية في مجال فرض حظر على تصدير الأسلحة الإلكترونية للدول والمناطق موضع النزاع.

١٧– أهمية التوازن بين الأمن والحرية في التعامل مع المخاطر الأمنية وتعزيز ثقافة حقوق الإنسان وحرية الرأي والتعبير في إطار من الحقوق والواجبات.

١٨- إن العمل على تشجيع دور الفضاء الإلكتروني في التنمية والإبداع والابتكار والنمو الاقتصادي من المهم للعمل على تعزيز الأهمية الاستراتيجية له، ودمج الطاقات العاطلة في التنمية وبخاصة بين الشباب.

نبذة عن المؤلف

الدكتور عادل عبد الصادق يعمل خبيرًا في مركز الأهـرام للدراسات السياسية والاستراتيجية، ومدير المركز العربي لأبحاث الفضاء الالكتروني. حصل على بكالوريوس الاقتصاد والعلوم السياسية من كلية الاقتصاد والعلوم السياسية بجامعة القاهرة، ثم حصل على درجة الماجستير في العلوم السياسية عام ٢٠٠٩ في موضوع «أثر الإرهاب الإلكتروني في مبدأ استخدام القوة في العلاقات الدولية»، وحصل على درجة الدكتوراه في العلوم السياسية في موضوع «أثر الفضاء الإلكتروني في تغيير طبيعة العلاقات الدولية: دراسة في النظرية والتطبيق»، من جامعة القاهرة – كلية الاقتصاد والعلوم السياسية عام ٢٠١٤.

تمتد فترة اهتمامه بأبحاث الفضاء الإلكتروني ما يزيد على ١٣ عامًا، ويهتم بالعديد من القضايا مثل دراسة الإرهاب الإلكتروني والاقتصاد الرقمي وحوكمة الإنترنت والتهديدات غير التقليدية للأمن ودراسات الإنترنت والمجتمع، والقانون الدولي، والعلوم السياسية في المجال الإلكتروني. وكان قد أسس مشروع المركز العربي لأبحاث الفضاء الإلكتروني في عام ٢٠٠٩، وشارك في تأسيس المنتدى العربي لحوكمة الإنترنت في بيروت ٢٠١٢.

حصل على جائزة أفضل مشروع ثقافي عربي عام ٢٠١١ وجائزة الشيخ سالم العلي الصباح للمعلوماتية، وحصل أيضًا في عام ٢٠١٠ على جائزة كتاب الجمهورية في تكنولوجيا الاتصال والمعلومات عن بحث «الديموقراطية الرقمية والدور السياسي للإنترنت في العالم العربي» في مايو ٢٠١٠، والترشح لجائزة دبي للصحافة عام ٢٠٠٨ عن دراسة «الإنترنت ساحة جديدة للتجسس الدولي»، وحصل على جائرة برنامج الأمم المتحدة لحقوق الإنسان عام ٢٠٠٧ عن تقرير «المدونات نمط جديد من المشاركة السياسة». وشارك عبد الصادق في العديد من المؤتمرات الدولية والعربية وفي وسائل الإعلام المسموعة والمرئية، وصدر له العديد من المقالات والأبحاث والكتب في مجال أبحاث الفضاء الإلكتروني.

قائمة المراجع

أولاً: المراجع العربية

أ- الوثائق

- «اتفاقيات جنيف ١٩٤٩ وبروتوكولاتها الإضافية». **اللجنة الدولية للصليب الأحمر.**

https://www.icrc.org/ara/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm

[تاريخ الدخول على الموقع: ١٧ أغسطس ٢٠١٦]

- «اتفاقية الأمم المتحدة لقانون البحار». **الأمم المتحدة.**

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N82/269/96/IMG/N8226996.pdf?OpenElement

[تاريخ الدخول على الموقع: ١٧ أغسطس ٢٠١٦]

- «الإعلان العالمي لحقوق الإنسان». **الأمم المتحدة.**

http://www.un.org/ar/documents/udhr

[تاريخ الدخول على الموقع: ١٧ أغسطس ٢٠١٦]

- الأمم المتحدة. مكتب شئون الفضاء الخارجي. **معاهدات الأمم المتحدة ومبادئها المتعلقة بالفضاء الخارجي: وقرارات الجمعية العمومية والوثائق الأخرى ذات الصلة.** د.م.، د.ت. كتاب إلكتروني متاح عبر الإنترنت.

http://www.unoosa.org/pdf/publications/ST_SPACE_51A.pdf

[تاريخ الدخول على الموقع: ١٧ أغسطس ٢٠١٦]

- القمة العالمية لمجتمع المعلومات. **الوثائق الصادرة عن القمة: جنيف ٢٠٠٣ – تونس ٢٠٠٥.** د.م.: الاتحاد الدولي للاتصالات، ٢٠٠٥. كتاب إلكتروني متاح عبر الإنترنت.
https://www.itu.int/net/wsis/outcome/booklet-ar.pdf
[تاريخ الدخول على الموقع: ١٧ أغسطس ٢٠١٦]

- «ميثاق الأمم المتحدة ٢٦ يونيو ١٩٤٥». **الأمم المتحدة.**
http://www.un.org/ar/charter-united-nations/index.html
[تاريخ الدخول على الموقع: ١٧ أغسطس ٢٠١٦]

ب– الكتب

- أبو الوفا، أحمد. **القانون الدولي للبحار على ضوء أحكام المحاكم الدولية والوطنية وسلوك الدول واتفاقية ١٩٨٢.** القاهرة: دار النهضة العربية، ٢٠٠٦.
- توفلر، ألفين. **تحول السلطة بين العنف والثروة والمعرفة.** ترجمة فتحي حمد بن شتوان، ونبيل عثمان. ليبيا: الدار الجماهيرية، ١٩٩٢.
- توفلر، ألفين. **صدمة المستقبل: المتغيرات في عالم الغد.** ترجمة محمد علي ناصف. تقديم أحمد كمال أبو المجد. ط. ٢. القاهرة: نهضة مصر، ١٩٩٠.
- حسين، مصطفى سلامة. **التأثير المتبادل بين التقدم العلمي والتكنولوجي والقانون الدولي.** القاهرة: دار النهضة العربية، ١٩٩٠.
- حلمي، نبيل أحمد. **القانون الدولي وفقًا لقواعد القانون الدولي العام.** القاهرة: دار النهضة العربية، ١٩٩٩.
- **دراسات في القانون الدولي الإنساني.** تقديم مفيد شهاب. القاهرة: دار المستقبل العربي، ٢٠٠٠.

- عبد الحي، وليد. **تحول المسلمات في نظريات العلاقات الدولية: دراسة مستقبلية.** الجزائر: مؤسسة الشروق، ١٩٩٤.
- عبد الرحمن، إسماعيل. «الأسس الأولية للقانون الإنساني الدولي». في **القانون الدولي الإنساني: دليل للتطبيق على الصعيد الوطني**، تقديم أحمد فتحي سرور. القاهرة: دار المستقبل العربي، ٢٠٠٣: ٢٠١–٣٤٠.
- عبد الصادق، عادل. **الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة.** القاهرة: مركز الأهرام للدارسات السياسية والاستراتيجية، ٢٠٠٩.
- عبد الصادق، عادل. **الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق.** القاهرة: المكتبة الأكاديمية، ٢٠١٦.
- عرجون، محمد بهي الدين. **الفضاء الخارجي واستخداماته السلمية.** عالم المعرفة ٢١٤. الكويت: المجلس الوطني للثقافة والفنون والآداب، ١٩٩٦.
- علوي، مصطفى. «مفهوم الأمن في مرحلة ما بعد الحرب الباردة». في **أبحاث المؤتمر الذي عقده مركز الدراسات الآسيوية ٤–٥ مايو ٢٠٠٢: قضايا الأمن في آسيا**، تحرير هدي ميتكيس، والسيد صدقي عابدين. القاهرة: جامعة القاهرة. كلية الاقتصاد والعلوم السياسية. مركز الدراسات الأسيوية، ٢٠٠٤.
- العناني، إبراهيم محمد. «المحكمة الجنائية الدولية ومنع انتشار أسلحة الدمار الشامل». الفصل الثالث في **الخيار النووي في الشرق الأوسط: أعمال الندوة الفكرية التي نظمها مركز دراسات المستقبل بجامعة أسيوط**، تحرير محمد إبراهيم منصور. بيروت: مركز دراسات الوحدة العربية، ٢٠٠١: ١٠٣–١١٩.
- غازي، خالد محمد. **الطوفان: العولمة: فك الثوابت وتحطيم الهويات.** القاهرة: دار الهدى، ١٩٩٨.

- **القانون الدولي الإنساني: دليل للتطبيق على الصعيد الوطني.** تقديم أحمد فتحي سرور. القاهرة: دار المستقبل العربي، ٢٠٠٣.
- كلارك، ريتشارد أ.، وروبرت نيك. **حرب الفضاء الإلكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه.** أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠١٢.
- كوبلاند، توماس إي. **ثورة المعلومات والأمن القومي.** دراسات عالمية ٤٦. أبوظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠٠٣.
- مقلد، إسماعيل صبري. **نظريات السياسة الدولية: دراسة تحليلية مقارنة.** ط. ٢. الكويت: ذات السلاسل، ١٩٨٧.
- ناي، جوزيف س. الابن. **المنازعات الدولية: مقدمة للنظرية والتاريخ.** ترجمة أحمد أمين الجمل، ومجدي كامل. القاهرة: الجمعية المصرية لنشر المعرفة والثقافة العالمية، ١٩٩٧.
- ناي، جوزيف س. **القوة الناعمة: وسيلة النجاح في السياسة الدولية.** ترجمة محمد توفيق البجيرمي. تقديم عبد العزيز عبد الرحمن الثنيان. الرياض: مكتبة العبيكان، ٢٠٠٤.
- ناي، جوزيف س. **مفارقة القوة الأمريكية: لماذا لا تستطيع القوة العظمى الوحيدة في العالم اليوم أن تنفرد في ممارسة قوتها.** ترجمة محمد توفيق البجيرمي. الرياض: مكتبة العبيكان، ٢٠٠٣.

ج- الدوريات

- «بوتين يُطلق سباق التسلّح مع الغرب». **الجزائر نيوز** (٢٠ فبراير ٢٠١٢). مقالة إلكترونية متاحة عبر الإنترنت.

http://www.djazairess.com/djazairnews/35239

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

- «دليل سان ريمو بشأن القانون الدولي المطبق في النزاعات المسلحة في البحار». **المجلة الدولية للصليب الأحمر**، العدد ٣٠٩ (٣١ ديسمبر ١٩٩٥). مقالة إلكترونية متاحة عبر الإنترنت.

https://www.icrc.org/ara/resources/documents/misc/5qzknh.htm

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

- دمج، أسامة. «أثر الأسلحة الجديدة على المدنيين». **مجلة الإنساني**، العدد ٣٥ (٢٠٠٦): ٢٦–٢٩.

- دي باولا، جيامباولو. «التحول في رؤيتنا للأمن مجلة حلف الناتو». **مجلة حلف الناتو**، العدد ٣ (٢٠٠٦). مقالة إلكترونية متاحة عبر الإنترنت.

http://www.nato.int/docu/review/2006/issue3/arabic/art2.html

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

- ستيوارت، جيمس ج. «نحو تعريف واحد للنزاع المسلح في القانون الدولي الإنساني: رؤية نقدية للنزاع المسلح المدوّل». **المجلة الدولية للصليب الأحمر**، العدد ٨٥٠ (٣١ ديسمبر ٢٠٠٣). مقالة إلكترونية متاحة عبر الإنترنت.

https://www.icrc.org/ara/resources/documents/misc/6ldja6.htm

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

- سلامة، صفات أمين. **أسلحة حروب المستقبل بين الخيال والواقع**. دراسات استراتيجية ١١٢. أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠٠٥.

«الصين تطور أسلحة جديدة قادرة على شل حركة حاملات الطائرات الأمريكية». **الصين بعيون عربية**.

http://www.chinainarabic.org/?p=3039

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]



- عبد الحميد، ريم. «الجارديان: الحكومة البريطانية تطور أسلحة هجوم إلكتروني». **اليوم السابع** (٣١ مايو ٢٠١١). مقالة إلكترونية متاحة عبر الإنترنت.

http://www.youm7.com/story/2011/5/31/424640/الجارديان--الحكومة-البريطانية-تطور-أسلحة-هجوم-إلكترونى
[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

- عبد السلام، محمد. «الحرب غير المتماثلة بين الولايات المتحدة والقاعدة». **مجلة السياسة الدولية**، العدد ١٤٧ (يناير ٢٠٠٢).
- عبد الصادق، عادل. «الإنترنت والاتصالات ساحة جديدة للتجسس الدولي». **قضايا استراتيجية** (يونيو ٢٠١٣).
- عبد الصادق، عادل. «الإنترنت والدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وإيران». **مختارات إيرانية** (نوفمبر ٢٠١١).
- عبد الصادق، عادل. «الفضاء الإلكتروني والتحول في سياسات أجهزة الاستخبارات الدولية». **كراسات استراتيجية**، العدد ٢٤٧ (٢٠١٣).
- عبد الصادق، عادل. «القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني». **مجلة السياسة الدولية**، العدد ١٨٨ (إبريل ٢٠١٢).
- عبد الصادق، عادل. «أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني: هل بدأ الاستعداد لحروب المستقبل؟» **السكينة**.

http://www.assakina.com/news/news1/9379.html
[تاريخ الدخول على الموقع: ١٦ أغسطس ٢٠١٦]

- عبد الصادق، عادل. «موقع ويكيليكس وتحدي عالم الاستخبارات الأمريكي». **ملف الأهرام الاستراتيجي**، العدد ١٩١ (أكتوبر ٢٠١٠).

- عبد الصادق، عادل. «هل يمثل الإرهاب الإلكتروني شكلاً جديدًا من أشكال الصراع الدولي». **ملف الأهرام الاستراتيجي**، العدد ١٥٦ (ديسمبر ٢٠٠٧).
- فيريليو، بول. «القنبلة المعلوماتية». ترجمة عادل حدجامي، وسعيد توبير. **مجلة فكر ونقد**، العدد ٢٩ (٢٠٠٦). مقالة إلكترونية متاحة عبر الإنترنت.

http://www.fikrwanakd.aljabriabed.net/n29_14hajjami.%282%29.htm

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

المرهون، عبد الجليل زيد. «عصر الردع الإلكتروني». **الجزيرة. نت**.

http://www.aljazeera.net/2FC311D7-4DFD-41E6-93FD-64B5C7A8C1D9/ForceRequestingFullContent/2FC311D7-4DFD-41E6-93FD-64B5C7A8C1D9/knowledgegate/opinions/2012/10/26/%d8%b9%d8%b5%d8%b1-%d8%a7%d9%84%d8%b1%d8%af%d8%b9-%d8%a7%d9%84%d8%a5%d9%84%d9%83%d8%aa%d8%b1%d9%88%d9%86%d9%8a/

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

د- رسائل علمية غير منشورة

- الدراجي، إبراهيم زهير. **جريمة العدوان ومدى المسئولية القانونية الدولية عنها**. رسالة دكتوراه. جامعة عين شمس. كلية الحقوق، ٢٠٠٢.
- شتا، أحمد عبد الونيس علي. **الدولة العاصية: دراسة في التعارض بين مواقف الدول والتزاماتها الدولية في الأمم المتحدة مع إشارة خاصة إلى إسرائيل وجنوب إفريقيا**. رسالة دكتوراه. جامعة القاهرة. كلية الاقتصاد والعلوم السياسية، ١٩٨٦.
- صادق، علي صادق عبد الحميد. **أمن الدولة في النظام القانوني للهواء والفضاء الخارجي**. رسالة دكتوراه. جامعة القاهرة. كلية الحقوق، ١٩٧٩.

- غلاب، سعيد حسين محمود حسن. **التطورات الراهنة في النظام الدولي وأثرها على مبدأ حظر استخدام القوة في العلاقات الدولية**. رسالة دكتوراه. جامعة القاهرة. كلية الاقتصاد والعلوم السياسية، ٢٠٠٥.
- قنديل، عابدين عبد الحميد حسن. **التدابير المضادة في النظام القانوني الدولي: دراسة نظرية وتطبيقية**. رسالة دكتوراه. جامعة القاهرة. كلية الاقتصاد والعلوم السياسية، ٢٠٠٦.
- مصطفى، منى محمود. **الجوانب القانونية والسياسية لمشاكل الفضاء الخارجي**. رسالة دكتوراه. جامعة القاهرة. كلية الاقتصاد والعلوم السياسية، ١٩٧٥.

هـ- أبحاث في ندوات

- شتا، أحمد عبد الونيس. «القانون الدولي والأسلحة النووية». في **أعمال ندوة إخلاء منطقة الشرق الأوسط من أسلحة الدمار الشامل: الجوانب القانونية**. القاهرة: جامعة القاهرة. كلية الاقتصاد والعلوم السياسية، ٢٠٠٤.

و- مواقع الإنترنت

- **الاتحاد الدولي للاتصالات.**

http://www.itu.int/ar/pages/default.aspx

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

- **الأمم المتحدة.**

http://www.un.org/ar/index.html

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

- **اللجنة الدولية للصليب الأحمر.**

https://www.icrc.org/ar

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

• **محكمة العدل الدولية.**

http://www.icj-cij.org/homepage/ar/

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

• **المركز العربي لأبحاث الفضاء الإلكتروني.**

www.accronline.com

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

• **منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو).**

http://ar.unesco.org/

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

• **منظمة العفو الدولية.**

https://www.amnesty.org/ar/

[تاريخ الدخول على الموقع: ٣ أغسطس ٢٠١٦]

ثانيًا: المراجع الأجنبية

A- Documents

- Council of Europe. *Convention on Cybercrime*. European Treaty Series, no. 185 (Budapest: Council of Europe, 2001). Online e-book.

  http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [accessed 17 Aug 2016]

- United Nations. *Charter of the United Nations: And Statue of the International Court of Justice*. San Francesco, 1945. Online e-book.

  https://treaties.un.org/doc/publication/ctc/uncharter.pdf [accessed 17 Aug 2016]

- "Geneva Conventions and Commentaries". *International Committee of the Red Cross*.

  https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions [accessed 17 Aug 2016]

- United Nations. *United Nations Convention on the Law of the Sea*. 1982. Online e-book.

  http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf [accessed 17 Aug 2016]

B: Official Resources

Books

- Adkins, Bonnie N. *The Spectrum of Cyber Conflict from Hacking to Information Warfare: What Is Law Enforcement's Role*? Alabama: Air University. Air Command and Staff College, 2001.

- Betts, Richard K. *Conflict after the Cold War: Arguments on Causes of War and Peace*. 2nd ed. New York: Longman, 2002.

- Ellis, Bryan W. *The International Legal Implications and Limitations of Information Warfare: What Are Our Options*? Pennsylvania: U.S. Army War College. Carlisle Barracks, 2001.
- Goldstein, Guy-Philippe. *Cyberspace and National Security: Selected Articles*. Edited by Gabi Siboni. Isreal: The Institute for National Security Studies, 2013. Online e-book.

  http://www.inss.org.il/uploadImages/systemFiles/CyberENG3925062787.pdf [accessed 4 Aug 2016]
- Gompert, David C., Irving Lachow, and Justin Perkins. *Battle-Wise Seeking Time-Information Superiority in Networked Warfare*. Washington, DC: Center for Technology and National Security Policy, 2006.
- Greenberg, Lawrence. T., Seymour E. Goodman, and Kevin J. Soo Hoo. *Information Warfare and International Law*. Washington, DC: National Defense University Press, 1998. Online e-book.

  http://www.iwar.org.uk/law/resources/iwlaw/iwilindex.htm [accessed 17 Aug 2016]
- Gumahad, Arsenio T. *Cyber Troops and Net War: The Profession of Arms in the Information Age*. Alabama: Air University. Air War College, 1996.
- Held, David, *et al. Global Transformations: Politics, Economics, and Culture*. California: Stanford University Press, 1999.
- Helm, Anthony M., ed. *The Law of War in the 21st Century: Weaponry and the Use of Force*. International Law Studies 82. Newport, Rhode Island: Naval War College, 2006.
- Hosek, James R., *et al. Attracting the Best: How the Military Competes for Information Technology Personnel*. Santa Monica, CA: RAND, 2004.
- Jordan, Tim. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London: Routledge, 2000.
- Karatzogianni, Athina, ed. *Cyber-Conflict and Global Politics*. Contemporary Security Studies. London: Routledge, 2008.

- Kugler, Richard L. "From Cyber Space to Cyber Power: Defining the Problems". Chapter. 2 in *Cyber Power and National Security*, edited by Franklin D. Krammer, Stuart Starr and Larry K. Wentz. National Defense University Series. Washington, DC: Center for Technology and National Security Policy, 2009.
- Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007.
- Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. Cass Series: Strategy and History 9. New York: Frank Cass, 2004.
- Mele, Stefano. *Cyber Weapon: Legal and Strategic Aspects. (Version 2.0)*. Rome: Italian Institute of Strategic Studies "Niccolò Machiavelli", 2013. Online e-book.

  http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf [accessed 4 Aug 2016]
- Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.
- Robinson, Neil, *et al. Stocktaking Study of Military Cyber Defense Capabilities in the European Union (milCyberCAP): Unclassified Summary*. RAND Corporation Research Report 286. Santa Monica, CA: RAND Corporation, 2013.
- Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown, 2012.
- Sheldon, John B. "Achieving Mutual Comprehension: Why Cyberpower Matters to Both Developed and Developing Countries". *Confronting Cyberconflict*, edited by Kerstin Vignard, vol. 4. Geneva: United Nations, 2001.
- Shulman, Mark Russell. *Legal Constraints on Information Warfare*. Occasional Paper Series 7. Alabama: Air University, Center for Strategy and Technology, 1999. Online e-book.

  www.au.af.mil/au/awc/awcgate/cst/csat7.pdf [accessed 3 Aug 2016]
- Tellis, Ashley J, *et al. Measuring National Power in the Postindustrial Age*. California: RAND, 2000.

- Vadnais, Daniel M. *Law of Armed Conflict and Information Warfare—How Does the Rule Regarding*: *Reprisals Apply to an Information Warfare Attack*? Alabama: Air Command and Staff College. The Research Department, 1997.
- Williamson, Jennie M. *Information Operations: Computer Network Attack in the 21st Century*. Strategy Research Project. Pennsylvania: US Army War College. Carlisle Barracks, 2002.

Newspapers

- Alexander, Keith B. "Warfighting in Cyberspace". *Joint Forces Quarterly* 3, no. 46 (2007): 58-61. Online e-article.

  http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-46.pdf [accessed 4 Aug 2016]
- Broad, William. J., John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay". *The New York Times* (15 Jan 2011). Online e-article.

  http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&pagewanted=all [accessed 3 Aug 2016]
- Coleman, Kevin G. "The Challenge of Unrestricted Warfare-A Look Back and a Look Ahead". *Directions Magazine*.

  http://www.directionsmag.com/entry/the-challenge-of-unrestricted-warfare-a-look-back-and-a-look-ahead/123237 [accessed 4 Aug 2016]
- Coleman, Kevin G. "Coleman: The Cyber Arms Race has Begun". *CSO* (28 Jan 2008). Online e-article.

  http://www.csoonline.com/article/2122353/critical-infrastructure/coleman--the-cyber-arms-race-has-begun.html [accessed 4 Aug 2016]
- Coleman, Kevin G. "Cyber Intelligence: Cyber Arms Race Is Well Underway". *Breaking Government* (9 Sep 2011). Online e-article.

  http://breakinggov.com/2011/09/09/cyber-intelligence-blog-cyber-arms-race-is-well-underway/ [accessed 4 Aug 2016]

- "Cyber Warfare Subject to Western Hegemony". *Global Times* (25 Mar 2013). Online e-article.

  http://www.globaltimes.cn/content/770576.shtml#.Ugao-KxlfFw [accessed 3 Aug 2016]

- Farnsworth, Timothy. "Is There a Place For Nuclear Deterrence in Cyberspace?" *Arms Control Now: The Blog of the Arms Control Association* (30 May 2013). Online e-article.

  https://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace/ [accessed 7 Aug 2016]

- Fouché, Morgane, Robert Macrae, and Jon Danielsson. "Could a Cyber Attack Cause a Financial Crisis?" *World Economic Forum* (13 June 2016). Online e-article.

  https://www.weforum.org/agenda/2016/06/could-a-cyber-attack-cause-a-financial-crisis [accessed 4 Aug 2016]

- Gjelten, Tom. "Is All The Talk About Cyberwarfare Just Hype?" *GBP News*.

  http://www.gpb.org/news/2013/03/15/is-all-the-talk-about-cyberwarfare-just-hype [accessed 4 Aug 2016]

- Glenny, Misha. "A Weapon We Can't Control". *The New York Times* (24 June 2012). Online e-article.

  http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html?_r=0 [accessed 7 Aug 2016]

- Glenny, Misha. "The Cyber Arms Race Is on, as Nations Large and Small Mobilize to Protect Themselves and Their Enemies if Provoked". *Pittsburgh Post-Gazette*.

  http://www.post-gazette.com/pg/11296/1183849-109-0.stm#ixzz1oMTYghXF [accessed 4 Aug 2016]

- Goldman, Zachary K. "Washington's Secret Weapon Against Chinese Hackers: Applying the Lessons of Counterterrorism and Counterproliferation in Cyberspace". *Foreign Affairs* (8 Apr 2013). Online e-article.

  https://www.foreignaffairs.com/articles/united-states/2013-04-08/washingtons-secret-weapon-against-chinese-hackers [accessed 4 Aug 2016]

- Goodman, J. David. “Iran Blocks American “Virtual Embassy”. *The New York Times* (7 Dec 2011). Online e-article.

  http://thelede.blogs.nytimes.com/2011/12/07/iran-blocks-american-virtual-embassy/ [accessed 3 Aug 2016]

- Grauman, Brigid. “Cyber-Security: The Vexed Question of Global Rules”. *Friends of Europe*.

  http://www.friendsofeurope.org/security-europe/3110/ [accessed 4 Aug 2016]

- Greenberg, Andy. “Shopping for Zero-Days: A Price List for Hackers’ Secret Software Exploits”. *Forbes* (23 Mar 2012). Online e-article.

  http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits [accessed 4 Aug 2016]

- Iran National CERT (MAHER). “Identification of a New Targeted Cyber-Attack”. *Embeddedsw*.

  http://embeddedsw.net/doc/New_targeted_cyber-attack.html [accessed 4 Aug 2016]

- “Iran Says Stuxnet Virus Infected 16,000 Computers”. *Fox News: World* (18 Feb 2012). Online e-article.

  http://www.foxnews.com/world/2012/02/18/iran-says-stuxnet-virus-infected-16000-computers/#ixzz1ntBzAB47 [accessed 3 Aug 2016]

- “Japan Developing Cyber Weapon: Report”. *The Australian Business Review* (2 Jan 2012). Online e-article.

  http://www.theaustralian.com.au/business/technology/japan-developing-cyber-weapon-report/story-e6frgakx-1226234630603 [accessed 4 Aug 2016]

- “Latest Snowden Leak: US Mounted 231 Cyber-Attacks Against Russia, Iran, and China”. *The Voice of Russia* (31 Aug 2012). Online e-article.

  http://sputniknews.com/voiceofrussia/news/2013_08_31/Latest-Snowden-leak-US-mounted-231-cyber-attacks-against-Russia-Iran-and-China-0260/ [accessed 4 Aug 2016]

- Markoff, John. “Vast Spy System Loots Computers in 103 Countries”. *The New York Times* (28 Mar 2009). Online e-article.

  http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=2&hpw [accessed 4 Aug 2016]

- McMillan, Robert. “Was Stuxnet Built to Attack Iran’s Nuclear Program?”. *PC World*.

  http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html [accessed 3 Aug 2016]

- Nakashima, E. “U.S. Accelerating Cyberweapon Research”. *The Washington Post*. Online e-article.

  https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html [accessed 4 Aug 2016]

- Nakashima, Ellen. “List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare”. *The Washington Post* (1 June 2011). Online e-article.

  https://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_print.html [accessed 4 Aug 2016]

- “Nuke Plant Sabotaged in High Tech Strike”. *The Day :News to Open Minds* (18 Jan 2011). Online e-article.

  http://theday.co.uk/technology/nuke-plant-sabotaged-in-high-tech-strike [accessed 4 Aug 2016]

- Patranobis, Sutirtho. “China Doesn’t Want Cyberspace Hegemony”. *Hindustan Times: Beijing* (June 2013). Online e-article.

  http://www.hindustantimes.com/world/china-doesn-t-want-cyberspace-hegemony/story-4rRyFbxLNhnpO2X9lod0BL.html [accessed 3 Aug 2016]

- Raywood, Dan. “US Says China and Russia Are Cyber Threats”. *CRN News*. http://www.crn.com.au/News/279216,us-says-china-and-russia-are-cyber-threats.aspx [accessed 4 Aug 2016]

- Shamah, David. "Digital World: Israel or 'Palestine'?" *The Jerusalem Post* (18 Mar 2008). Online e-article.

  http://www.jpost.com/Health-and-Sci-Tech/Internet-And-Technology/Digital-World-Israel-or-Palestine [accessed 7 Aug 2016]

- Traynor, Ian. "Russia Accused of Unleashing Cyber War to Disable Estonia". *The Guardian* (17 May 2007). Online e-article.

  https://www.theguardian.com/world/2007/may/17/topstories3.russia [accessed 7 Aug 2016]

- "U.S. Launches 'Virtual' Embassy for Iran". *US Today News* (12 June 2011). Online e-article.

  http://www.usatoday.com/news/washington/story/2011-12-06/us-embassy-iran/51673966/1 [accessed 3 Aug 2016]

- "United Nations: Recent Developments in the Field of Information and Telecommunications in the Context of International Security". *NATO Cooperative Cyber Defence Centre of Excellence: Incyder News* (14 Nov 2012) Online e-article.

  https://ccdcoe.org/united-nations-recent-developments-field-information-and-telecommunications-context-international.html [accessed 7 Aug 2016]

Reports

- Foreign and International Law Committee of the New York County Lawyers' Association "NYCLA". *Report of the Foreign and International Law Committee of the New York County Lawyers' Association on the Unlawfulness of the Use and Threat of Use of Nuclear Weapons.* New York: NYCLA, 2000. Online e-report.

  http://www.nuclearweaponslaw.com/JournalsReport/NYCLA_Report.pdf. [accessed 8 Aug 2016]

- Mulvenon, James C. *Chinese Information Operations Strategies in a Taiwan Contingency*. Washington, DC: US-China Economic and Security Review Commission, 2005. Online e-report.

http://origin.www.uscc.gov/sites/default/files/9.15.05mulvenon.pdf [accessed 4 Aug 2016]

- Peake, Adam. Internet Governance and the World Summit on the Information Society (WSIS). N.p.: Association for Progressive Communications (APC), 2004. Online e-report.

  https://www.apc.org/en/system/files/governance.pdf [accessed 8 Aug 2016]

- Smith, Craig. *The World Wide Web of War*. Pennsylvania: US Army War College, 2006. Online e-report.

  http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA449402&Location=U2&doc=GetTRDoc.pdf [accessed 8 Aug 2016]

- Stein Schjølberg. *Report of the Chairman of HLEG*. ITU Global Cybersecurity Agenda (GCA), International Telecommunication Union. Online e-report.

  https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf [accessed 17 Aug 2016]

- Transparency Market Research. *Cyber Weapon Market – Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2015–2021*. 2015. Online e-report.

  http://www.transparencymarketresearch.com/cyber-weapon-market.html [accessed 7 Aug 2016]

- UNESCO. *Towards Knowledge Societies: For Peace and Sustainable Development, First WSIS+10 Review Meeting*. Paris: UNESCO, 2013. Online e-report.

  http://www.unesco.org/D08582F1-17E1-4A92-B9E5-9A0EBDFAFB89/FinalDownload/DownloadId-CCBBF0CEB595FA7D26EBB375487BA4DC/D08582F1-17E1-4A92-B9E5-9A0EBDFAFB89/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_outcomes_en.pdf [accessed 8 Aug 2016]

- USA. Department of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*. USA: Office of the Secretary of Defense, 2013. Online e-report.

  http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf [accessed 7 Aug 2016]

- Wilson, Clay. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Washington, DC: Congressional Research Service, 2008. Online e-report.

  https://www.fas.org/sgp/crs/terror/RL32114.pdf [accessed 8 Aug 2016]

Periodicals

- Carpenter, Ted Galen. “The New World Disorder”. *Foreign Policy*, no. 84 (1991): 24-39.
- Cohen, Daniel, and Aviv Rotbart. “The Proliferation of Weapons in Cyberspace”. *Military and Strategic Affairs* 5, no. 1 (May 2013): 59-61. Online e-article.

  http://www.inss.org.il/uploadImages/systemFiles/MASA5-1Eng4_Cohen%20and%20Rotbart.pdf [accessed 3 Aug 2016]
- Delibasis, Dimitrios. “State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century”. *Peace Conflict and Development*, no. 8 (Feb 2006).
- Dunn, Myriam A. “Information Age Conflicts: A Study of the Information Revolution and a Changing Operating Environment”. *Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung,* no. 64 (2002). Online e-article.

  http://kms1.isn.ethz.ch/serviceengine/Files/ISN/55/ipublicationdocument_singledocument/dadc0d4d-948f-4d9d-8b54-fce922e1f152/en/doc_57_290_en.pdf [accessed 3 Aug 2016]
- Dunn, Myriam A. “The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method”. *Information and Security: An International Journal* 7 (2001): 145-158. Online e-article.

  http://procon.bg/system/files/07.08_Dunn.pdf [accessed 3 Aug 2016].
- Khan, Zafar. “Strategizing Cyber Revolution within the Domain of Security Studies”. *IPRI Journal* 15, no. 2 (Summer 2015): 95-112. Online e-article.

  http://www.ipripak.org/wp-content/uploads/2015/10/5-art-s-15.pdf [accessed 3 Aug 2016]

- Rowe, N.C. “War Crimes from Cyber-Weapons”. *The Journal of Information Warfare* 6, no. 3 (Dec 2007):15-25.
- Reynolds, Jefferson D. “Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground”. *Air Force Law Review* 56 (2005): 1-108.
- De Never, Renee. “Modernizing the Geneva Conventions”. *The Washington Quarterly* 29, no. 2 (2006).
- Schmitt, Michael N. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”. *Columbia Journal of Transnational Law* 37 (1998): 885-937.
- Schmitt, Michael N. “Wired Warfare: Computer Network Attack and Jus in Bello”. *IRRC* 84, no. 846 (June 2002): 365-400. Online e-article.

  https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf [accessed 1 Aug 2016]
- Shulman, Mark R. “Discrimination in the Laws of Information Warfare”. *The Columbia Journal of Transnational Law* 37, no. 3 (1999): 937-998.
- Stevens, Tim. “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace”. *Contemporary Security Policy* 33, no. 1 (2012): 148-170.
- Walsh, Lucas, and Julien Barbara. “Speed, International Security, and “New War” Coverage in Cyberspace”. *Journal of Computer-Mediated Communication* 12, no. 1 (Oct 2006): 189–208. Online e-article.

  http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2006.00321.x/full [accessed 3 Aug 2016]
- Wenger, Andreas. “The Internet and the Changing Face of International Relations and Security”. *Information and Security: An International Journal* 7 (2001): 5-11.

Conferences

- DeWeese, Geoffrey S. "Anticipatory and Preemptive Self-defense in Cyberspace: the Challenge of Imminence". *7th International Conference on Cyber Conflict. Proceedings 2015*, edited by M. Maybaum, A.M. Osula and L. Lindström. NATO Cooperative Cyber Defence Centre of Excellence, 2015. Online e-book.

  https://ccdcoe.org/cycon/2015/proceedings/06_deweese.pdf [accessed 3 Aug 2016]

Internet Resources

- Bieber, Florian. "Cyberwar or Sideshow? The Internet and the Balkan Wars", *Current History* 99, no. 635 (Mar 2000): 124-128. Online e-article.

  http://search.proquest.com/docview/200751259?accountid=7180 [accessed 3 Aug 2016]

- Dörmann, Knut. "Applicability of the Additional Protocols to Computer Network Attacks". *International Committee of the Red Cross*.

  https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf [accessed 7 Aug 2016]

- Dörmann, Knut. "Computer Network Attack and International Humanitarian Law". *International Committee of the Red Cross*.

  https://www.icrc.org/eng/resources/documents/article/other/5p2alj.htm [accessed 7 Aug 2016]

- Freed, Anthony M. "US Defense Budget to Both Regulate and Proliferate Cyber Weapons". *Tripwire: The State of Security*.

  http://www.tripwire.com/state-of-security/top-security-stories/us-defense-budget-regulate-proliferate-cyber-weapons/ [accessed 7 Aug 2016]

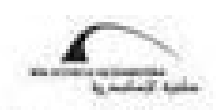
- Paganini, Pierluigi. “The Rise of Cyber Weapons and Relative Impact on Cyberspace”. *InfoSec Institute*.

  http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/ [accessed 4 Aug 2016]

- Walsh, Eddie. “The Cyber Proliferation Threat”. *The Diplomat*.

  http://thediplomat.com/2011/10/the-cyber-proliferation-threat/ [accessed 4 Aug 2016]


BIBLIOTHECA ALEXANDRINA
مكتبة الإسكندرية



وحدة الدراسات المستقبلية

للاستعلام

تليفون: ٤٨٣٩٩٩٩ (٢٠٣)+ داخلي: ١٢٨٨

فاكس: ٤٨٧٩٢٥٢ (٢٠٣)+

الموقع الإلكتروني: www.bibalex.org

ISBN: 978-977-452-366-1